Thornton v. May demonstrates just how difficult it is to manage and expunge personal information. PAGE 24

Sun CEO Jonathan Schwartz and CIO Louis Quintero back use of the Open Document Format PAGE 7

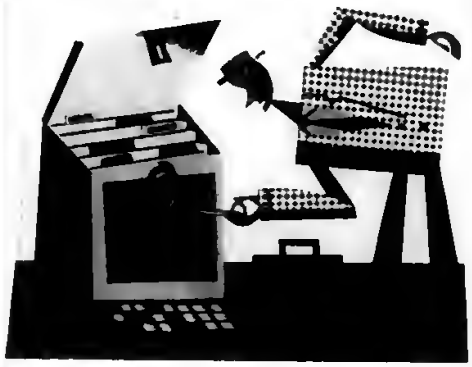
COMPUTERWORLD

THE VOICE OF IT MANAGEMENT ■ WWW.COMPUTERWORLD.COM

APRIL 17, 2006 ■ VOL 40 ■ NO 16 ■ $5/COPY

KNOWLEDGE CENTER **SECURITY**

The Business of Security



IT leaders are taking a more businesslike approach to security. They're using cost-benefit analyses, dashboards and data classification to ensure that security dollars are spent on the biggest risks. **Stories begin on page 27.**

PUBLIC EXPOSURE

Counties Post Personal Data in Documents

Online records put Social Security numbers, other sensitive info in open

BY JAIKUMAR VIJAYAN

BROWARD COUNTY, Fla., Fort Bend County, Texas, and Maricopa County, Ariz., have something in common: In recent years, they have made sensitive personal information about their residents, such as Social Security, driver's license and bank account numbers, available to anyone in the world with Internet access.

And they aren't alone by any means. The failure to remove sensitive data from images of land records and other public documents posted online has made county government Web sites across the U.S. a veritable treasure trove of information for identity thieves and other criminals, several privacy advocates claimed last week.

Go to our Web site to read full coverage of data breaches and other IT security and privacy issues

"These sites are just spoon-feeding criminals the information they need," said BJ Ostergren, a Virginia resident who runs a privacy-related Web site called The Virginia Watchdog.

The pieces of personally identifiable information found on county Web sites and made available to *Computerworld* by Ostergren and other privacy advocates included the Social

Personal Data, page 10

IT Execs Take Different Routes on Bird Flu Threat

Fears of an outbreak prompt continuity planning by some; others see no need

BY MATT HAMBLEN

The answer to the question of whether corporate IT departments would be ready to respond if an avian flu pandemic hit the U.S. is: Maybe.

Based on interviews last week with 13 CIOs, business continuity directors and IT management consultants, U.S. companies continue to hold widely divergent views on the risk that a flu outbreak could force school closings or broad quarantines in hard-hit areas.

Some IT leaders, mainly at large companies, said they are preparing for the worst in an effort to avoid being left short-staffed or unable to support vastly increased numbers of telecommuters on their networks if a pandemic strikes.

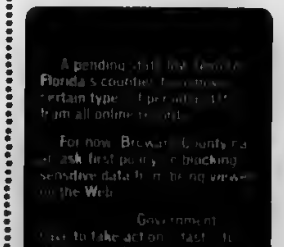
CIO has been preparing for a pandemic for six months

For example, Beneficial Financial Group in Salt Lake City "is seriously looking into the pandemic issue," said CIO Steve Terry. "Since we are a life insurance company, [being prepared] makes sense for us. We have to have the capability to continue doing business if there is a pandemic."

In contrast, several other

Bird Flu, page 56

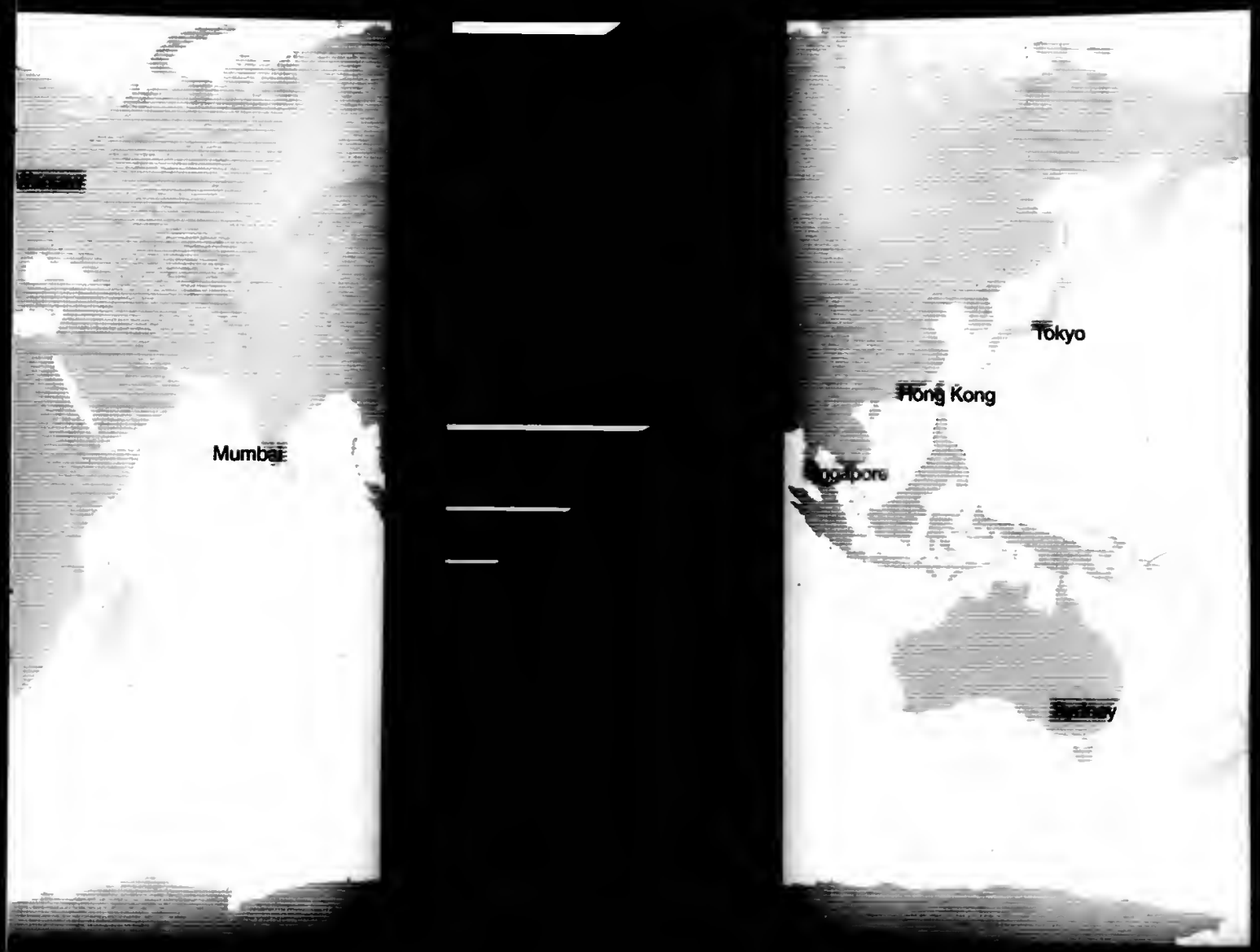
> **"In my estimation, 'do nothing' is not a good solution because it leaves the information out there for public viewing."**
>
> BRUCE HOGMAN, IT PROFESSIONAL AND RESIDENT OF BROWARD COUNTY, FLORIDA



THE WORLD ACCORDING TO

MAYA

att.com/networking

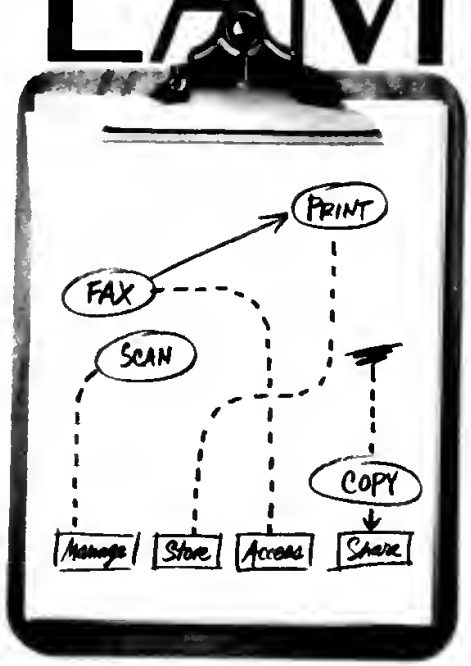


I have people to support and ideas to enable. Look out world, because my network is coming through.

Dynamic Networking from AT&T gives Maya the IP solutions she needs to connect suppliers, customers and employees worldwide. With IP VPNs, Maya has a cost-effective networking solution that allows users to collaborate no matter where they are. And with AT&T's integrated network security, Maya knows she can expand her endpoints without any increase in exposure.

The new at&t

TEAM PLAYER



Global companies have teams everywhere. To help them share ideas, Xerox multifunction systems and software put everyone on the same playing field. There's a new way to look at it.

Running a global company requires secure worldwide information sharing. Luckily, Xerox has a solution for everyone on your team. Using Xerox multifunction systems and Xerox DocuShare® software, documents can be securely scanned to the Web. This way people throughout your global network can share them. This keeps documents current, can eliminate warehousing needs by 70% and can reduce order fulfillment time by 80%. Whatever Xerox WorkCentre® multifunction system you choose, you'll reduce costs by printing, copying, scanning and faxing from one convenient network device. Now that's a game plan. To learn more, contact us today.

XEROX.

xerox.com/office/team
1-800-ASK-XEROX ext. 753

Technology | Document Management | Consulting Services

CONTENTS

04.17.06

NEWS

ONLINE

ONLINE DEPARTMENTS

Breaking News
computerworld.com/news

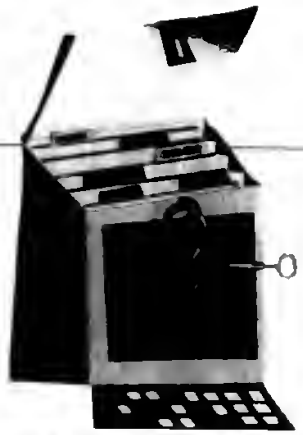
Newsletter Subscriptions
computerworld.com/newsletters

Knowledge Centers
computerworld.com/topics

The Online Store
computerworld.com/store

OPINIONS

DEPARTMENTS/RESOURCES



KNOWLEDGE CENTER SECURITY

The Business of Security. Savvy IT leaders are taking a more business-like approach to security. They're using cost-benefit analyses, dashboards and data classification schemes to match investments to the biggest risks. **Package starts on page 27.**

The following related content can be found online at computerworld.com/security.

IT Management Survey
Computerworld polled 671 IT professionals about their organizations' security practices. View the results to better understand how your peers view security technologies and management issues, ranging from budgets to restrictions on portable storage media.

Webcast
Biometric authentication is widely regarded as the most foolproof of authentication systems. This webcast will give an overview of biometrics and some of the key issues IT professionals should be aware of when evaluating this technology.

AT DEADLINE

Offshore Boom Benefits Infosys

Infosys Technologies Ltd., riding a boom in offshore outsourcing, reported that its revenue had surpassed $2 billion for its fiscal year ended March 31. Bangalore, India-based Infosys reported revenue of $2.15 billion for the year, up by 35% over revenue of $1.6 billion in fiscal 2005. Profits for the year rose 32%, to $555 million. Infosys has forecast sales growth of 28% to 30% in fiscal 2007.

CA to Buy Software Vendor for $75M

CA Inc. has agreed to buy Cybermation Inc., a maker of enterprise workload automation software, for $75 million. Islandia, N.Y.-based CA said it will add Cybermation's tools to its workload automation offerings. A privately held company based in Markham, Ontario, Cybermation reported revenue of about $30 million in 2005. CA expects the deal to close within 30 days.

AMD's Q1 Revenue And Profits Improve

Advanced Micro Devices Inc. reported healthy increases in sales and profits in its first quarter, which ended March 26. Strong demand for dual-core processors led to record sales of AMD's Opteron processor in the quarter.

		PROFIT/LOSS
Q1 '06	$1.33B	$185M
Q1 '05	$1.23B	($37M)

DHL Names Former GM Exec as CIO

DHL International Ltd. has named Maryann Goebel CIO of DHL Express for the Americas, the Asia-Pacific region and emerging markets/Latin America. Goebel, who previously was CIO at General Motors North America, will oversee all DHL IT initiatives in those regions. Goebel reports to John Mullen, joint chief executive of DHL Express, and will be based at DHL's U.S. corporate headquarters in Plantation, Fla.

Lawson Users Aren't Sure About Upgrading

Next-generation apps require new IT infrastructure

BY MARC L. SONGINI
ORLANDO

LAWSON SOFTWARE Inc. users last week expressed mixed feelings about upgrading to the company's next-generation Lawson 9 and Landmark applications, with some citing fears that the migration requires excessive technology changes.

The comments from users at Lawson's Customer and User Exchange 2006 conference here last week came as the company unveiled the first piece of its Landmark ERP system.

The Landmark Strategic Sourcing application, introduced less than a month after Lawson brought out Version 9 of its application suite, aims to improve and automate the procurement process.

Lawson officials declined to disclose further delivery plans for the Landmark line, which will succeed Lawson 9.

The city government of Greensboro, N.C., plans to begin using the new Strategic Sourcing software this fall, several months after it installed the Lawson 9 financial and human resources software. The city was an early adopter of the Lawson 9 applications, which were officially introduced last month.

Chryste Hover, the municipality's director of ERP, said the decision to use Lawson 9 required that the city first install the IBM WebSphere-based Lawson System Foundation 9, which is also needed to run Landmark applications.

Hover said that the technology requirement entailed some work for the city's IT operation, since it had to swap out its Microsoft Internet Information Service Web server for WebSphere. Greensboro also had to upgrade its IBM AIX-based pSeries hardware and Oracle Corp. database software to support the new system, she said.

"You need to be on the cutting-edge, technologically, [to upgrade to Lawson 9]," Hover explained.

The technology requirements are causing Wilsons The Leather Experts Inc. in Brooklyn Park, Minn., to take "a wait-and-see attitude with Lawson 9.0 and Landmark," said Scott Christian, the retailer's director of business systems. Wilson is upgrading from Lawson 7 to Lawson 8 ERP software.

Christian said that the technology requirement for upgrading to the new versions entails "a significant change and one that I'm not sure will deliver tangible business benefits for Wilsons Leather at this time. I also believe there is a level of risk involved in making the change right now that we are not willing to accept."

After viewing demonstrations of the initial Landmark offering at the user conference, Chuck Kentfield, senior software engineer for human resources at Pacific Life Insurance Co. in Newport Beach, Calif., called it "a solid improvement in technology."

Kentfield said he expects to migrate from Version 9 to Landmark but can't set a timetable for that until Lawson discloses its delivery plans.

The Strategic Sourcing application has attracted the interest of Sandi Klos, business project manager for materials management at HealthPartners Medical Group and Clinics in St. Paul, Minn.

The health services provider currently runs Version 8 of Lawson's procurement, payroll and human resources applications. Klos said she expects HealthPartners to install Lawson System Foundation 9 by 2007.

Predrag Jakovljevic, an analyst at Montreal-based research firm Technology Evaluation Centers Inc., said user response to the significant architectural changes that are needed to use Landmark remains unclear.

Jakovljevic said the WebSphere requirement might not suit customers who are standardized around Windows-based products.

ACQUISITION WORRIES

Despite Lawson's planned merger with Intentia, users still worry that the former may be purchased by another company

www.computerworld.com

Lawson CEO Weighs In on Landmark, Intentia Plans

ORLANDO

Harry Debes, president and CEO of Lawson Software, has overseen development of the next-generation Landmark application set and the company's acquisition of Danderyd, Sweden-based ERP software vendor Intentia International AB, due to close this month. Debes spoke about the acquisition, Lawson's technology focus and the ERP business in an interview with Computerworld last week.

Has the agreement to buy Intentia caused any of your customers to have doubts about the future? It's been more of an issue for Intentia customers than Lawson's, in direct correlation to being the acquired company versus the acquirer. We've tried to be consistent and send a message that really hasn't changed over the last 12 months. That is, these products serve different markets, the personnel are different, and we want to keep them both alive and have continuity.

Why were you chosen to lead Lawson at the same time the company agreed to buy Intentia? Think about the Intentia merger. I had done a lot of mergers and acquisition work in my previous history. I had also done international work. Before joining Lawson, I spent about 50% of my time working globally.

Can Lawson stay competitive against ERP giants like Oracle and SAP? You can be smaller and nimbler and find segments not well served by the giants.

You can do things with customers [that] they'd never get from SAP. You spend time with smaller firms face to face, building relationships. Our whole client experience isn't just a bullet on a PowerPoint slide.

We plan to do about eight or nine verticals and get really, really good at those. We don't need to be in a 150 countries. We don't want to do technology or middleware – just applications. We'll surround that software with a whole range of value-added services.

What is the status of Lawson's new Landmark applications? We kept it fairly quiet and didn't offer a lot of marketing hype around Landmark. We said to the developers, "Let's get real and make this happen." The good news is [the Landmark developers] have done everything we asked them and more, and it's not necessary to be that cautious now. We're not scrapping all the legacy code we have, and we still have a lot of customers using our existing core systems, and we'll continue enhancing them as we bring out new modules in Landmark.

Does Lawson plan to offer hosted applications? There's so much talk about online software, and I scratch my head and wonder where it's coming from. I rarely get questions by customers about it. However, we are going to offer a hosted human-capital management service by midsummer and see what happens.

– MARC L. SONGINI

Red Hat Again Tries to Move Beyond OS Level

Planned purchase of JBoss gives Linux vendor new hope in app server market

BY ERIC LAI AND HEATHER HAVENSTEIN

Red Hat Inc.'s planned acquisition of application server vendor JBoss Inc. is its third attempt to move up the open-source software stack in a big way. And it's hoping that this time proves to be the charm.

Red Hat has had limited success at getting users to adopt the directory server software it launched last June and a Java-based application server that it released in 2004. But some IT managers applauded its proposed marriage with JBoss.

"Of all the potential firms that could have acquired JBoss, we feel that Red Hat — being an open-source proponent — is a good match for us," said Barry Strasnick, CIO at CitiStreet LLC, a Quincy, Mass., company that manages benefits programs for companies and government agencies.

CitiStreet, which formerly was a big user of BEA Systems Inc.'s WebLogic application server, started moving to the open-source JBoss technology two years ago. Now the company uses JBoss on top of Red Hat Linux to support all of its mission-critical applications, Strasnick said.

Badri Nittoor, CEO of JBoss systems integrator Tripod Technologies LLC in Cherry Hill, N.J., said the acquisition will move Red Hat closer to having an enterprise-class stack of open-source software.

But he added that it remains to be seen how well the cultures of the two companies will mesh, since JBoss has more control over the source code for its software than Red Hat does over Linux.

Raleigh, N.C.-based Red Hat said it agreed to pay at least $350 million in cash and stock for Atlanta-based JBoss. It added that the price tag could rise to $420 million if JBoss meets certain financial targets under Red Hat's ownership.

Red Hat unveiled its Directory Server software, bought from America Online Inc.'s Netscape division, at its first user conference last spring.

Stiff Competition

But that market is dominated by Microsoft Corp.'s Active Directory, followed by Novell Inc.'s eDirectory software, said Sara Radicati, principal analyst at The Radicati Group Inc. in Palo Alto, Calif. Red Hat's market share "is very small, let's put it that way," she said.

Red Hat also offers an application server based on the open-source Jonas technology developed by the ObjectWeb Consortium in Montbonnot, France. Red Hat CEO Matthew Szulik said during a conference call last week that the company has made "a significant investment in Jonas, and we expect that to continue."

But Laurent Lachal, an analyst at London-based Ovum Ltd., said Red Hat has been disappointed by the adoption of Jonas and is unlikely to devote a lot of resources to that technology once it owns JBoss.

About half of the JBoss user base runs the application server on Windows. That could complicate Red Hat's marketing strategy, said Steve Walli, a vice president at Optaros Inc., an open-source consulting firm in Boston.

On the other hand, Jason Long, CEO and chief software engineer at Supernova Software Inc. in Houston, said the JBoss deal might motivate him to switch his company's internal applications from Windows to Red Hat Linux.

"This should lower that barrier and make it a more attractive option," said Long, who is also founder of the Houston JBoss Users Group. ■

Acquisition Plan

- Red Hat will make an initial payment of $140 million in cash plus stock valued at $210 million to buy JBoss.
- JBoss will become an independent division of Red Hat after the deal closes, which is expected in late May.
- Marc Fleury, CEO of JBoss, will continue to run the unit and will report to Red Hat CEO Matthew Szulik.

James Niccolai and China Martens of the IDG News Service contributed to this story.

New Mass. CIO Defends Open Document Plan

BY CAROL SLIWA

Massachusetts CIO **Louis Gutierrez** *said last week that he doesn't envision "a full-scale, completed implementation" of the state's controversial Open Document Format (ODF) policy by its January 2007 deadline. But in his first in-depth interview since Feb. 6, when he became CIO and director of the state's Information Technology Division (ITD) for the second time, Gutierrez told* Computerworld *that he also doesn't foresee the state taking a "wait position" with respect to the ODF policy, which applies to the government's executive branch. A status update on ODF is due by midyear, he noted. Excerpts from the interview follow:*

How committed are you to the Enterprise Technical Reference Model that the ITD announced in September and to the ODF policy that's part of it? One of the reasons that I was glad to take up the assignment to come back to ITD is that I do believe in the technical reference model objective, and I very much believe in the important role that the [division] has in promoting standards. I'm proud and grateful to promote and defend a standard like this.

Do you think your predecessors made a sound decision with respect to ODF? I do think that this was a far-seeing and very thoughtful objective, and I think that's one reason it has resonated the way it has. It has captured the essence of an important notion about openness, about standards, about the way documents are used and will be used.

I've signed up to do the execution, and I have a lot of work to do on implementation planning and on addressing concerns of accessibility advocates. But I do think this is the right direction to be going.

Is that based on a desire not to tie up documents in proprietary formats for the long haul? I would add a different angle on this. In the world of government work, we think of these documents as being somehow memos that individuals save to disk, and somehow we want those records to live a long time, and there might be a long thread of arguments around that. But truly, the records management topic is the prerogative of records management people, and I want to focus on the benefits to an executive department of state government. The world that we're entering is one of much more workflow of structured documents and knowing in great detail and controlling your document formats. Open-standard document formats are absolutely the future of where things are heading.

Microsoft doesn't support ODF and has raised objections about the policy. Have you been trying to work out a compromise? We're not talking about a compromise to the policy if Microsoft were able to work with ODF. One benefit of an open-standards policy is to allow much greater competition among office suites on the desktop. And furthermore, there are circumstances where low-cost and open-source office suites are the right solution, and other circumstances where Microsoft Office, were it to comply with the policy, would be appropriate as well.

Have you been trying to impress upon Microsoft the need for an ODF converter? We've been trying to impress upon them that our policy is not an anti-Microsoft policy, that we would be very interested in ODF converter capabilities for a number of reasons. It simplifies and makes less costly some of the implementation we would need to do. And it avoids months of question marks over whether Microsoft Office products will ultimately qualify under the policy.

How open are you to including Microsoft's Office Open XML file format as part of the policy, should its submission to Ecma International become a standard? We have not said that the policy will be restricted to only one standard over time. But we care very much that our policy objectives are met by whatever standard is looked at.

As to the moves that Microsoft has been making with regard to its own Open XML format, I think there has been progress. The move from legacy formats to XML formats, improved licensing and covenant not-to-sue provisions that apply to these formats, the submission of the format to a standards body, the incorporation of a "save to PDF" — these truly are positive movements. We are very encouraged by these things, and when a standardization process is complete, we'll look forward to evaluating the situation to see if it meets the policy requirements. ■

AT DEADLINE

Offshore Boom Benefits Infosys

Infosys Technologies Ltd., riding a boom in offshore outsourcing, reported that its revenue had surpassed $2 billion for its fiscal year ended March 31. Bangalore, India-based Infosys reported revenue of $2.15 billion for the year, up by 35% over revenue of $1.6 billion in fiscal 2005. Profits for the year rose 32%, to $555 million. Infosys has forecast sales growth of 28% to 30% in fiscal 2007.

CA to Buy Software Vendor for $75M

CA Inc. has agreed to buy Cybermation Inc., a maker of enterprise workload automation software, for $75 million. Islandia, N.Y.-based CA said it will add Cybermation's tools to its workload automation offerings. A privately held company based in Markham, Ontario, Cybermation reported revenue of about $30 million in 2005. CA expects the deal to close within 30 days.

AMD's Q1 Revenue And Profits Improve

Advanced Micro Devices Inc. reported healthy increases in sales and profits in its first quarter, which ended March 26. Strong demand for dual-core processors led to record sales of AMD's Opteron processor in the quarter.

QUARTER	REVENUE	NET INCOME (LOSS)
Q1 '06	$1.33B	$135M
Q1 '05	$1.23B	($17M)

DHL Names Former GM Exec as CIO

DHL International Ltd. has named Maryann Goebel CIO of DHL Express for the Americas, the Asia-Pacific region and emerging markets/Latin America. Goebel, who previously was CIO at General Motors North America, will oversee all DHL IT initiatives in those regions. Goebel reports to John Mullen, joint chief executive of DHL Express, and will be based at DHL's U.S. corporate headquarters in Plantation, Fla.

Lawson Users Aren't Sure About Upgrading

Next-generation apps require new IT infrastructure

BY MARC L. SONGINI
ORLANDO

LAWSON SOFTWARE Inc. users last week expressed mixed feelings about upgrading to the company's next-generation Lawson 9 and Landmark applications, with some citing fears that the migration requires excessive technology changes.

The comments from users at Lawson's Customer and User Exchange 2006 conference here last week came as the company unveiled the first piece of its Landmark ERP system.

The Landmark Strategic Sourcing application, introduced less than a month after Lawsoo brought out Version 9 of its application suite, aims to improve and automate the procurement process.

Lawson officials declined to disclose further delivery plans for the Landmark line, which will succeed Lawson 9.

The city government of Greensboro, N.C., plans to begin using the new Strategic Sourcing software this fall, several months after it installed the Lawson 9 financial and human resources software. The city was an early adopter of the Lawson 9 applications, which were officially introduced last month.

Chryste Hover, the municipality's director of ERP, said the decision to use Lawson 9 required that the city first install the IBM WebSphere-based Lawson System Foundation 9, which is also needed to run Landmark applications.

Hover said that the technology requirement entailed some work for the city's IT operation, since it had to swap out its Microsoft Internet Information Service Web server for WebSphere. Greensboro also had to upgrade its IBM AIX-based pSeries hardware and Oracle Corp. database software to support the new system, she said.

"You need to he on the cutting-edge, technologically, [to upgrade to Lawson 9]," Hover explained.

The technology requirements are causing Wilsons The Leather Experts Inc. in Brooklyn Park, Minn., to take "a wait-and-see attitude with Lawson 9.0 and Landmark," said Scott Christian, the retailer's director of business systems. Wilson is upgrading from Lawson 7 to Lawson 8 ERP software.

Christian said that the technology requirement for upgrading to the new versions entails "a significant change and one that I'm not sure will deliver tangible business benefits for Wilsons Leather at this time. I also believe there is a level of risk involved in making the change right now that we are not willing to accept."

After viewing demonstrations of the initial Landmark offering at the user conference, Chuck Kentfield, senior software engineer for human resources at Pacific Life Insurance Co. in Newport Beach, Calif., called it "a solid improvement in technology."

Kentfield said he expects to migrate from Version 9 to Landmark but can't set a timetable for that until Lawson discloses its delivery plans.

The Strategic Sourcing application has attracted the interest of Sandi Klos, business project manager for materials managemeot at HealthPartners Medical Group and Clinics in St. Paul, Minn.

The health services provider currently runs Version 8 of Lawsoo's procurement, payroll and buman resources applications. Klos said she expects HealthPartners to install Lawson System Foundation 9 by 2007.

Predrag Jakovljevic, an analyst at Montreal-based research firm Technology Evaluation Centers Inc., said user response to the significant architectural changes that are needed to use Landmark remains unclear.

Jakovljevic said the WebSphere requirement might not suit customers who are standardized around Windows-based products. ▸

ACQUISITION WORRIES

Despite Lawson's planned merger with Intentia, users still worry that the former may be purchased by another company
www.computerworld.com

Lawson CEO Weighs In on Landmark, Intentia Plans

ORLANDO

Harry Debes, president and CEO of Lawson Software, has overseen development of the next-generation Landmark application set and the company's acquisition of Denderyd, Sweden-based ERP software vendor Intentia International AB, due to close this month. Debes spoke about the acquisition, Lawson's technology focus and the ERP business in an interview with Computerworld last week.

Has the agreement to buy Intentia caused any of your customers to have doubts about the future? It's been more of an issue for Intentia customers than Lawson's, in direct correlation to being the acquired company versus the acquirer. We've tried to be consistent and send a message that really hasn't changed over the last 12 months. That is, these products serve different markets, the personnel are different, and we want to keep them both alive and have continuity.

Why were you chosen to lead Lawson at the same time the company agreed to buy Intentia? Think about the Intentia merger. I had done a lot of mergers and acquisition work in my previous history. I had also done international work. Before joining Lawson, I spent about 50% of my time working globally.

Can Lawson stay competitive against ERP giants like Oracle and SAP? You can be smaller and nimbler and find segments not well served by the giants.

You can do things with customers [that] they'd never get from SAP. You spend time with smaller firms face to face, building relationships. Our whole client experience isn't just a bullet on a PowerPoint slide.

We plan to do about eight or nine verticals and get really, really good at those. We don't need to be in a 150 countries. We don't want to do technology or middleware – just applications. We'll surround that software with a whole range of value-added services.

What is the status of Lawson's new Landmark applications? We kept it fairly quiet and didn't offer a lot of marketing hype around Landmark. We said to the developers, "Let's get real and make this happen." The good news is [the Landmark developers] have done everything we asked them and more, and it's not necessary to be that cautious now. We're not scrapping all the legacy code we have, and we still have a lot of customers using our existing core systems, and we'll continue enhancing them as we bring out new modules in Landmark.

Does Lawson plan to offer hosted applications? There's so much talk about online software, and I scratch my head and wonder where it's coming from. I rarely get questions by customers about it. However, we are going to offer a hosted human-capital management service by midsummer and see what happens.

– MARC L. SONGINI

Red Hat Again Tries to Move Beyond OS Level

Planned purchase of JBoss gives Linux vendor new hope in app server market

BY ERIC LAI AND HEATHER HAVENSTEIN

Red Hat Inc.'s planned acquisition of application server vendor JBoss Inc. is its third attempt to move up the open-source software stack in a big way. And it's hoping that this time proves to be the charm.

Red Hat has had limited success at getting users to adopt the directory server software it launched last June and a Java-based application server that it released in 2004. But some IT managers applauded its proposed marriage with JBoss.

"Of all the potential firms that could have acquired JBoss, we feel that Red Hat — being an open-source proponent — is a good match for us," said Barry Strasnick, CIO at CitiStreet LLC, a Quincy, Mass., company that manages benefits programs for companies and government agencies.

CitiStreet, which formerly was a big user of BEA Systems Inc.'s WebLogic application server, started moving to the open-source JBoss technology two years ago. Now the company uses JBoss on top of Red Hat Linux to support all of its mission-critical applications, Strasnick said.

Badri Nittoor, CEO of JBoss systems integrator Tripod Technologies LLC in Cherry Hill, N.J., said the acquisition will move Red Hat closer to having an enterprise-class stack of open-source software.

But he added that it remains to be seen how well the cultures of the two companies will mesh, since JBoss has more control over the source code for its software than Red Hat does over Linux.

Raleigh, N.C.-based Red Hat said it agreed to pay at least $350 million in cash and stock for Atlanta-based JBoss. It added that the price tag could rise to $420 million if JBoss meets certain financial targets under Red Hat's ownership.

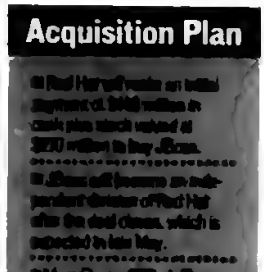
Red Hat unveiled its Directory Server software, bought from America Online Inc.'s Netscape division, at its first user conference last spring.

Stiff Competition

But that market is dominated by Microsoft Corp.'s Active Directory, followed by Novell Inc.'s eDirectory software, said Sara Radicati, principal analyst at The Radicati Group Inc. in Palo Alto, Calif. Red Hat's market share "is very small, let's put it that way," she said.

Red Hat also offers an application server based on the open-source Jonas technology developed by the ObjectWeb Consortium in Montbonnot, France. Red Hat CEO Matthew Szulik said during a conference call last week that the company has made "a significant investment in Jonas, and we expect that to continue."

But Laurent Lachal, an analyst at London-based Ovum Ltd., said Red Hat has been disappointed by the adoption of Jonas and is unlikely to devote a lot of resources to that technology once it owns JBoss.



About half of the JBoss user base runs the application server on Windows. That could complicate Red Hat's marketing strategy, said Steve Walli, a vice president at Optarus Inc., an open-source consulting firm in Boston.

On the other hand, Jason Long, CEO and chief software engineer at Supernova Software Inc. in Houston, said the JBoss deal might motivate him to switch his company's internal applications from Windows to Red Hat Linux.

"This should lower that barrier and make it a more attractive option," said Long, who is also founder of the Houston JBoss Users Group.

James Niccolai and China Martens of the IDG News Service contributed to this story.

New Mass. CIO Defends Open Document Plan

BY CAROL SLIWA

Massachusetts CIO **Louis Gutierrez** *said last week that he doesn't envision "a full-scale, completed implementation" of the state's controversial Open Document Format (ODF) policy by its January 2007 deadline. But in his first in-depth interview since Feb. 6, when he became CIO and director of the state's Information Technology Division (ITD) for the second time, Gutierrez told* Computerworld *that he also doesn't foresee the state taking a "wait position" with respect to the ODF policy, which applies to the government's executive branch. A status update on ODF is due by midyear, he noted. Excerpts from the interview follow:*

How committed are you to the Enterprise Technical Reference Model that the ITD announced in September and to the ODF policy that's part of it? One of the reasons that I was glad to take up the assignment to come back to ITD is that I do believe in the technical reference model objective, and I very much believe in the important role that the [division] has in promoting standards. I'm proud and grateful to promote and defend a standard like this.

Do you think your predecessors made a sound decision with respect to ODF? I do think that this was a far-seeing and very thoughtful objective, and I think that's one reason it has resonated the way it has. It has captured the essence of an important notion about openness, about standards, about the way documents are used and will be used.

I've signed up to do the execution, and I have a lot of work to do on implementation planning and on addressing concerns of accessibility advocates. But I do think this is the right direction to be going.

Is that based on a desire not to tie up documents in proprietary formats for the long haul? I would add a different angle on this. In the world of government work, we think of these documents as being somehow memos that individuals save to disk, and somehow we want those records to live a long time, and there might be a long thread of arguments around that. But truly, the records management topic is the prerogative of records management people, and I want to focus on the benefits to an executive department of state government. The world that we're entering is one of much more workflow of structured documents and knowing in great detail and controlling your document formats. Open-standard document formats are absolutely the future of where things are heading.

Microsoft doesn't support ODF and has raised objections about the policy. Have you been trying to work out a compromise? We're not talking about a compromise to the policy if Microsoft were able to work with ODF. One benefit of an open-standards policy is to allow much greater competition among office suites on the desktop. And furthermore, there are circumstances where low-cost and open-source office suites are the right solution, and other circumstances where Microsoft Office, were it to comply with the policy, would be appropriate as well.

Have you been trying to impress upon Microsoft the need for an ODF converter? We've been trying to impress upon them that our policy is not an anti-Microsoft policy, that we would be very interested in ODF converter capabilities for a number of reasons. It simplifies and makes less costly some of the implementation we would need to do. And it avoids months of question marks over whether Microsoft Office products will ultimately qualify under the policy.

How open are you to including Microsoft's Office Open XML file format as part of the policy, should its submission to Ecma International become a standard? We have not said that the policy will be restricted to only one standard over time. But we care very much that our policy objectives are met by whatever standard is looked at.

As to the moves that Microsoft has been making with regard to its own Open XML format, I think there has been progress. The move from legacy formats to XML formats, improved licensing and covenant not-to-sue provisions that apply to these formats, the submission of the format to a standards body, the incorporation of a "save to PDF" — these truly are positive movements. We are very encouraged by these things, and when a standardization process is complete, we'll look forward to evaluating the situation to see if it meets the policy requirements.

BRIEFS

Sun High-End Unit Cuts 200 Workers

Sun Microsystems Inc. has laid off about 200 people from its Scalable Systems Group. The layoffs represent about 7% of the group's workforce. Managers of the high-end systems division also streamlined the group by closing open requisitions, reallocating resources and increasing organizational efficiency.

Salesforce.com Buys Wireless Vendor

Salesforce.com Inc. has acquired wireless technology developer Sendia Corp. for $15 million in cash. Salesforce.com already uses Sendia technology in its AppExchange Mobile offering, which allows corporate customers to access on-demand applications using handheld computers and smart phones. Santa Monica, Calif.-based Sendia employs 35 workers.

McAfee Portal Offers Virus Information

McAfee Inc. has unveiled a new online portal called McAfee Threat center, which is designed to help users research a wide range of security problems. The portal will provide updates on viruses along with information from the company's Avert Labs division on topics such as spam, phishing and spyware. The site will also offer free tools, blogs and articles from McAfee security experts.

$2.65B Settlement Of AOL Suit OK'd

A judge approved a $2.65 billion settlement of a lawsuit brought against Time Warner Inc. by shareholders that alleged that America Online Inc. improperly accounted for revenue in the years preceding and following the AOL-Time Warner merger. Judge Shirley Wohl Kram of the U.S. District Court in New York ruled that the settlement of the class-action lawsuit is fair, reasonable and adequate. A Time Warner spokeswoman declined to comment on the settlement.

ON THE MARK

HOT TECHNOLOGY TRENDS, NEW PRODUCT NEWS AND INDUSTRY BUZZ BY MARK HALL

MATTHEW PAULSON

It's Time for Real Time . . .

. . . when it comes time to analyze customer data. There's a real-time deluge of customer information inside companies today, but it's difficult to make instant decisions about what the data means. William Hobbib, vice president of marketing at Lexington, Mass.-based StreamBase Systems Inc., thinks that will change with the release this week of his company's StreamBase 3.0 software. He says ao updated StreamBase Optimizer module runs queries on real-time information three times faster than the previous release did. CEO Barry Morris explains that StreamBase executes its real-time queries on "windows" of streaming data that are herded ioto relational tables in RAM. And given that StreamBase is a 64-bit app, it supports a lot of memory indeed. If a query needs historical information, StreamBase can yank it from a disk and put it into a data window. Pricing starts at $95,000.

But not all analytical data can be neatly organized in relational tables. That's why Intelligent Results Inc. in Bellevue, Wash., next week plans to unveil Predigy, an analytics software tool that not only dissects structured data for business intelligence clues but also cao be applied to unstructured information found in e-mails, Word files and other documeots. CEO Kelly Pennock claims that because Predigy can sift through both kinds of data, it's "better at predicting customer behavior." Pricing starts at $50,000.

Don't write out your company's app . . .

. . . requirements – draw them. Well, sort of. Marc Brown, senior director of product marketing at Borland Ioc., says the Cupertino, Calif.-based company's new Caliber DefineIT software lets tech-savvy husiness analysts "create graphical storyboards" — basically flow charts of their software specifications that "fully flesh out functional components." Brown says the tool's visual nature helps end users agree more quickly oo how an application should work. Caliber DefineIT costs $2,000 and is due on May 5.

Open-source subverts the dominant . . .

. . . development paradigm. In the future, you won't be managing a significant software development project that doesn't involve programmers strewn about the planet. So why use tools that were designed for people working side by side? asks Bill Portelli, CEO of CollabNet Inc. in Brisbane, Calif. That's why his firm has become the primary sponsor of Subversion, an open-source version-control tool designed for developers working together over the Web. This week, CollabNet unveils its Subversion On-Demand service, which adds collaboration, lifecycle management and other features on a subscription basis. CollabNet charges $33,000 per year for 50 development team members.

On-demand software can be pricey . . .

. . . compared with perpetual license approaches. "There's a little bit of sticker shock when you look long term," says Benjamin Holtz, CEO of Green Beacon LLC io Watertown, Mass. For example, to get "true costs," he suggests that you compare on-demand software with licensed applications over a period of three to five years. The licensed approach wins every time, Holtz claims. Still, his company, which customizes packaged CRM and ERP apps, faces competitive pressure from the likes of Salesforce.com Inc. because price isn't the only reason users like the on-demand model. Letting someone else manage the software is another. So Green Beacon has devised a hosted alternative for CRM users, starting at $6,000 per month. In the fall, Green Beacon will offer ERP software in a hosted environment, Holtz says.

Federal foot-dragging on data privacy . . .

. . . legislation hurts businesses. Without a national privacy protection law to abide by, U.S. IT vendors are at a disadvantage against their European and Japanese competitors. That's the assertion of Phil Dunkelberger, CEO of PGP Corp. in Palo Alto, Calif. He says the fragmented, state-driven privacy policies in the U.S. give pause to European and Japanese governments and businesses that are evaluating U.S. technologies and services. "They wonder whether our government is serious about protecting private information," Dunkelberger says. "The perception is that here in the U.S., we are not diligent about protecting data." He adds that PGP, which offers data security tools to IT users, doesn't have a preference among any of the dozen or so privacy bills circulating in Congress.

"We just need to get one to the floor for a vote," says Dunkelberger, who testified this month on the urgency for passing such legislation. But congressional staffers tell him that any privacy bill "is a long shot for 2006," he says. Election year and all that. So when your representative is campaigning locally instead of doing the people's busioess in Washington, give him an earful about the need for a federal data-privacy bill — now.

AMD

power of cool

Continued from page 1

Personal Data

Security number of Rep. Tom Delay (R-Texas) on a tax lien document; the Social Security numbers of Florida Gov. Jeb Bush and his wife on a quitclaim deed from 1999; the driver's license numbers, vehicle registration information, height, race and addresses of people arrested for traffic violations; the names and birth dates of minors from divorce decrees; and complete copies of death certificates.

"All of this information is available to anyone sitting in a cafe in Nigeria or anywhere else in the world," said David Bluys, a retired private investigator who publishes a newsletter called "News for County Officials" in Shallowater, Texas. "It's a real security threat."

Scope of Threat Unknown

It's hard to say exactly how many of the 3,600 county governments around the country are posting sensitive data on the Web, said Mark Monacelli, president of the Property Records Industry Association, a Durham, N.C.-based industry group set up to facilitate the recording of and access to public property information.

But it's safe to assume that a large number of them are, said Darity Wesley, CEO of La Mesa, Calif.-based Privacy Solutions Inc., which offers consulting services to the real estate industry. "I think a lot of [county] recorders have been putting public land records on the Internet without any concern about who has access to them," Wesley said.

Sue Baldwin, director of the Broward County Records Division in Florida, said all of the state's counties are subject to a law requiring them to maintain Web sites for public records, many of which contain sensitive data.

A new Florida statute requires counties by the start of next year to black out Social Security, bank account, and credit and debit card numbers from document images that are already posted online. Also starting on Jan. 1, county recorders will be given the authority to black out the same numbers from new documents.

For now, recorders have "no statutory authority to automatically remove" such information from documents, Baldwin said. She added that Broward County residents who want sensitive data immediately excised from public records must file written requests.

Baldwin and Carol Fogelsong, the assistant comptroller for Florida's Orange County, both downplayed the privacy and security issues of making full images of records available online, noting that anyone can view the actual documents at county offices.

"I understand people's concerns, but a lot of this information has been freely available for public inspection since Plymouth Rock," Fogelsong said.

"This is not a new situation," Baldwin said, pointing out that Broward County began posting documents online in 1999. And because records have been publicly available "since the beginning of time," concerns about posting them on the Internet amount to "a tempest in a teapot," she said.

> I understand people's concerns, but a lot of this information has been freely available for public inspection since Plymouth Rock.
>
> CAROL FOGELSONG
>
> These sites are just spoon-feeding criminals the information they need.
>
> BJ OSTERGREN

Wesley and Monacelli acknowledged that the availability of personal information online raises justifiable privacy concerns. But those worries need to be tempered by an understanding of the benefits, such as easier access to land records, they said.

"This whole topic of access to information is an issue that we as a nation are facing," Monacelli said. "We have real estate professionals, title companies, attorneys and lenders who need this information for commerce purposes."

There is also little evidence to show that the public availability of personal information on government sites has contributed to an increase in identity theft, Wesley said. For most identity thieves, the chore of sifting through millions of public records for useful data simply isn't worth the effort, she added.

Instead of wrapping "a lot of fear and sensationalism" around the issue, Wesley said, what is needed is an informed discussion among legislators, privacy advocates and business representatives. She has organized a working group, with 20 members from the private and public sectors, to create model legislation governing the redaction of Social Security numbers and other personal data from records.

The number of public documents that contain sensitive information may be far lower than people assume, according to Fogelsong. Orange County is using an outside company to inspect about 30 million pages dating back to 1970 for the data that needs to be removed under Florida's new statute (see related story, below). Fogelsong said that 119,000 of the 7 million pages inspected thus far have needed to have data hidden from view, or redacted.

The number of redacted pages amounts to just 1.63% of the total that have been inspected, Fogelsong noted. However, she added, the percentage is expected to go up to about 5% in the case of older documents because many more of them are likely to contain sensitive information.

Baldwin said there is also less sensitive data than meets the eye on Broward County's Web site. "Most people's documents don't have [that kind of] stuff in them," she said.

However, critics such as Bluys and Ostergren dismissed arguments that public records have long been available in pa-

Continued on page 12

Florida Counties Face State Deadline on Hiding Numbers

LIKE OTHER counties in Florida, Orange County is scrambling to comply with a state mandate that requires Social Security, bank account, and credit and debit card numbers to be removed by the start of 2007 from all online images of public records.

For Orange County, it's an enormous task that involves examining nearly 30 million page images from records dating back to 1970, said Carol Fogelsong, the county's assistant comptroller.

Instead of trying to do the work itself, Orange County last June signed a contract with Hart InterCivic Inc., an Austin-based provider of records management services for county governments.

Since then, the county has downloaded onto USB drives images of about 25 million pages from documents dated through April 30, 2005, and shipped them to Hart for inspection and redaction.

Hart has inspected about 7 million pages thus far and found information that needed to be redacted on about 119,000 of them, Fogelsong said.

Pages containing redactions are loaded back onto USB drives and returned to Orange County, which then replaces the original image with the new page. Fogelsong said the original images aren't actually deleted – they're just hidden from view.

Despite initial concerns about the technology challenges, the redaction process has been going better than expected, according to Fogelsong. She said Hart is using specialized optical character recognition (OCR) software to look for the banned numbers on both handwritten and typed pages. The pages are also being manually reviewed to ensure that nothing is missed, she added.

About 2 million pages are now being inspected per month, Fogelsong said. The process costs the county 2.35 cents per page, which would add up to a tab of $705,000 for the full allotment of 30 million pages.

Fogelsong acknowledged that even after the work is completed, some online documents will likely still display information that is supposed to be hidden. "I will not be able to stop everything," she said. "But I'm doing the best I can."

Florida's Broward County plans to do its redaction work internally using software it bought from Aptitude Solutions Inc. in Casselberry, Fla., said Sue Baldwin, director of the Broward County Records Division.

"I don't know how long the actual process will take," she said. "But we intend to comply with the statutory requirements, including [the] deadline."

According to Baldwin, there are "relatively few documents" posted on the county's Web site that include sensitive information. Nonetheless, she said, the required redaction effort is "a massive job. We can't do it overnight."

Bruce Hogman, a Broward County resident who has worked as an IT professional for the past 30 years, said the effectiveness of OCR tools in redaction efforts could be limited by the challenges involved in programming the software to recognize specific types of data in documents that use different formats and are of varying quality.

As a result, the redaction of sensitive data could take longer than expected, leaving information publicly available for the next several months, Hogman said. He also noted that because much of the information already has been viewable for quite some time, it is questionable how useful redacting the data will be.

– JAIKUMAR VIJAYAN AND KEN MINGIS

Continued from page 1

Personal Data

Security number of Rep. Tom Delay (R-Texas) on a tax lien document; the Social Security numbers of Florida Gov. Jeb Bush and his wife on a quitclaim deed from 1999; the driver's license numbers, vehicle registration information, height, race and addresses of people arrested for traffic violations; the names and birth dates of minors from divorce decrees; and complete copies of death certificates.

"All of this information is available to anyone sitting in a café in Nigeria or anywhere else in the world," said David Bloys, a retired private investigator who publishes a newsletter called "News for County Officials" in Shallowater, Texas. "It's a real security threat."

Scope of Threat Unknown

It's hard to say exactly how many of the 3,600 county governments around the country are posting sensitive data on the Web, said Mark Monacelli, president of the Property Records Industry Association, a Durham, N.C.-based industry group set up to facilitate the recording of and access to public property information.

But it's safe to assume that a large number of them are, said Darity Wesley, CEO of La Mesa, Calif.-based Privacy Solutions Inc., which offers consulting services to the real estate industry. "I think a lot of [county] recorders have been putting public land records on the Internet without any concern about who has access to them," Wesley said.

Sue Baldwin, director of the Broward County Records Division in Florida, said all of the state's counties are subject to a law requiring them to maintain Web sites for public records, many of which contain sensitive data.

A new Florida statute requires counties by the start of next year to black out Social Security, bank account, and credit and debit card numbers from document images that are already posted online. Also starting on Jan. 1, county recorders will be given the authority to black out the same numbers from new documents.

For now, recorders have "no statutory authority to automatically remove" such information from documents, Baldwin said. She added that Broward County residents who want sensitive data immediately excised from public records must file written requests.

Baldwin and Carol Fogelsong, the assistant comptroller for Florida's Orange County, both downplayed the privacy and security issues of making full images of records available online, noting that anyone can view the actual documents at county offices.

"I understand people's concerns, but a lot of this information has been freely available for public inspection since Plymouth Rock," Fogelsong said.

"This is not a new situation," Baldwin said, pointing out that Broward County began posting documents online in 1999. And because records have been publicly available "since the beginning of time," concerns about posting them on the Internet amount to "a tempest in a teapot," she said.

I understand people's concerns, but a lot of this information has been freely available for public inspection since Plymouth Rock.

These sites are just spoon-feeding criminals the information they need.

Wesley and Monacelli acknowledged that the availability of personal information online raises justifiable privacy concerns. But those worries need to be tempered by an understanding of the benefits, such as easier access to land records, they said.

"This whole topic of access to informatioo is an issue that we as a nation are facing," Monacelli said. "We have real estate professionals, title companies, attorneys and lenders who need this information for commerce purposes."

There is also little evidence to show that the public availability of personal information on government sites has contributed to an increase in identity theft, Wesley said. For most identity thieves, the chore of sifting through millions of public records for useful data simply isn't worth the effort, she added.

Instead of wrapping "a lot of fear and sensationalism" around the issue, Wesley said, what is needed is an informed discussion among legislators, privacy advocates and business representatives. She has organized a working group, with 20 members from the private and public sectors, to create model legislation governing the redaction of Social Security numbers and other personal data from records.

The number of public documents that contain sensitive information may be far lower than people assume, according to Fogelsong. Orange County is using an outside company to inspect about 30 million pages dating back to 1970 for the data that needs to be removed under Florida's new statute (see related story, below). Fogelsong said that 119,000 of the 7 million pages inspected thus far have needed to have data hidden from view, or redacted.

The number of redacted pages amounts to just 1.63% of the total that have been inspected, Fogelsong noted. However, she added, the percentage is expected to go up to about 5% in the case of older documents because many more of them are likely to contain sensitive information.

Baldwin said there is also less sensitive data than meets the eye on Broward County's Web site. "Most people's documents don't have [that kind of] stuff in them," she said.

However, critics such as Bloys and Ostergren dismissed arguments that public records have long been available in pa-

Continued on page 12

Florida Counties Face State Deadline on Hiding Numbers

LIKE OTHER counties in Florida, Orange County is scrambling to comply with a state mandate that requires Social Security, bank account, and credit and debit card numbers to be removed by the start of 2007 from all online images of public records.

For Orange County, it's an enormous task that involves examining nearly 30 million page images from records dating back to 1970, said Carol Fogelsong, the county's assistant comptroller.

Instead of trying to do the work itself, Orange County last June signed a contract with Hart InterCivic Inc., an Austin-based provider of records management services for county governments.

Since then, the county has downloaded onto USB drives images of about 25 million pages from documents dated through April 30, 2005, and shipped them to Hart for inspection and redaction.

Hart has inspected about 7 million pages thus far and found information that needed to be redacted on about 119,000 of them, Fogelsong said.

Pages containing redactions are loaded back onto USB drives and returned to Orange County, which then replaces the original image with the new page. Fogelsong said the original images aren't actually deleted – they're just hidden from view.

Despite initial concerns about the technology challenges, the redaction process has been going better than expected, according to Fogelsong. She said Hart is using specialized optical character recognition (OCR) software to look for the banned numbers on both handwritten and typed pages. The pages are also being manually reviewed to ensure that nothing is missed, she added.

About 2 million pages are now being inspected per month, Fogelsong said. The process costs the county 2.35 cents per page, which would add up to a tab of $705,000 for the full allotment of 30 million pages.

Fogelsong acknowledged that even after the work is completed, some online documents will likely still display information that is supposed to be hidden. "I will not be able to stop everything," she said. "But I'm doing the best I can."

Florida's Broward County plans to do its redaction work internally using software it bought from Aptitude Solutions Inc. in Casselberry, Fla., said Sue Baldwin, director of the Broward County Records Division.

"I don't know how long the actual process will take," she said. "But we intend to comply with the statutory requirements, including [the] deadline."

According to Baldwin, there are "relatively few documents" posted on the county's Web site that include sensitive information. Nonetheless, she said, the required redaction effort is "a massive job. We can't do it overnight."

Bruce Hagreen, a Broward County resident who has worked as an IT professional for the past 30 years, said the effectiveness of OCR tools in redaction efforts could be limited by the challenges involved in programming the software to recognize specific types of data in documents that use different formats and are of varying quality.

As a result, the redaction of sensitive data could take longer than expected, leaving information publicly available for the next several months, Hagreen said. He also noted that because much of the information already has been viewable for quite some time, it is questionable how useful redacting the data will be.

– JAIKUMAR VIJAYAN AND KEN MINGIS

AMD

power of cool

BRIEFS

Oracle Buys Billing Software Vendor

Oracle Corp. last week agreed to buy Portal Software Inc., a maker of billing and revenue management software for the communications industry, for about $220 million. Oracle expects the transaction to close in June and plans to integrate Portal's software capabilities into its ERP applications and the CRM software it acquired with Siebel Systems Inc. Oracle said it may use Portal's software for other industries.

Sun Adds Microsoft Link to Thin Clients

Sun Microsystems Inc. has rolled out the second generation of its Sun Ray thin-client devices and software with added links to Windows environments. The new offerings also include smart-card slots to enable "hot desking," which allows the use of Java-based cards to switch devices on the fly, starting up sessions where they left off.

NetApp to Expand Indian Operations

Network Appliance Inc. plans to expand a development center in Bangalore, India, that builds and supports several product lines, including its NetCache product. The center is also likely to run the company's worldwide information systems. The expansion will include a new 180,000-square-foot facility that will house about 750 engineers over the next two years.

IBM Builds Chip Encryption Tool

IBM researchers have developed encryption technology that can be built directly into a microprocessor to help lock down data in mobile phones, PDAs, digital media players and other devices. The technology, called Secure Blue, can be used in consumer electronics, medical and government applications, and digital media. IBM is building the technology into its Power processor. The technology will also work in other vendors' processors.

Continued from page 10

Personal Data

per form as specious.

"The simple truth is these records were safe in the courthouse for 160 years," Bloys said. Now all it takes is Internet access and a rudimentary idea of how to look for sensitive data to find all sorts of information, he added.

Ostergren claimed that simply by "messing around" on county Web sites over the past three and a half years, she has found hundreds of thousands of pages containing sensitive information. She has printed out more than 17,000 records containing people's Social Security numbers, the maiden names of their mothers (often used to verify identities) and the names of minors.

Among the countless nuggets that Bloys said he has found online was the complete medical history of a terminally ill government official in the Texas county of Fort Bend.

Buying Data in Bulk

It isn't always necessary to search through Web sites, because online records can often be purchased in bulk for a fraction of what it would cost to buy them at a courthouse, Bloys said. For example, he said, officials in Fort Bend County last year sold a Florida company online copies of every document ever filed with the county clerk's office. The cost for the estimated 20 million documents was about $2,500, said Bloys, who wrote an article about the transaction in his newsletter.

A call seeking comment on the matter from the Fort Bend County recorder's office hadn't been returned as of *Computerworld*'s publication deadline.

The company that bought the information is among a large number of businesses — including some in India, China and the Philippines — that routinely download records directly from county Web sites, Bloys claimed.

Bruce Hogman, a Broward County county resident who recently raised concerns about the posting of personally identifiable information with Baldwin's office, said real estate professionals and other business users don't need all of the information included in documents posted online.

For real estate transactions, Hogman said, "they need nothing more than the names of the parties, the date of the transaction, the consideration, the book and page in which the data is recorded, together with the legal description — and not the actual image of the documents themselves."

Ostergren said efforts to stop Virginia's Hanover County, where she lives, from posting images of public records online have succeeded so far. But 14 of the state's 121 cities and counties do make records available online, she said, adding that the same thing is being done by counties in states such as Pennsylvania, North and South Carolina, Ohio, Georgia, Arizona, Texas and New York. That includes all five boroughs in New York City, according to Ostergren.

Fogelsong noted that Orange County residents who want information removed from documents can request that it be redacted (see related story, below). "I would love if people would check their records on their own" to ensure that no private data is publicly disclosed, she said.

But Ostergren dismissed such advice, saying Florida and North Carolina are currently the only states that allow residents to ask for their Social Security numbers to be removed from online records that were already posted.

On the other hand, many states have given county clerks the power to refuse to record new documents containing personally identifiable data, Ostergren said. Overall, though, "this online records mess has been the best-kept secret," she added. "Ninety-nine percent of citizens haven't a clue that the records are online in the first place."

Computerworld's Ken Mingis contributed to this story.

Redaction Tools Hunt For, Hide Personal Information

REDACTION SOFTWARE works in much the same way that antispam tools do – by using algorithms to look for specific phrases or words. But they analyze images, not e-mail.

Some vendors use multiple levels of automatic analysis, while others narrow down the number of documents likely to need redaction and then rely on human intervention to help improve the software's automatic redaction capabilities.

"It's a new technology, but a proven technology," said Paul Miller, president of Aptitude Solutions Inc. in Casselberry, Fla. Miller said Aptitude's aiRedact software looks for specific numbers, words or combinations of related words, such as "account number" or "Social Security number."

On big jobs involving millions of document images, several thousand pages are culled and manually analyzed by a worker who can verify that data should be redacted, Miller said. The software then automatically adjusts to redact the remaining records based on the manual choices. It typically costs between $200,000 and $300,000, he said.

ImageTech Systems Inc. in Camp Hill, Pa., has built a plug-in redaction module for Kofax Ascent Capture, a tool from Kofax Image Products Inc. in Irvine, Calif., that finds data in documents and forms.

R.J. Oommen, ImageTech's principal, said the plug-in module uses several methods, including on-the-fly input from users, automatic processing of data in standard forms and an intelligent algorithm. The module starts at $5,000, but the total cost can exceed $100,000, Oommen said.

Other redaction vendors include SRS Technologies' Systems Technology Group, Appligent Inc. and Image Architects Inc.

– TODD R. WEISS

Data Removal Is a Private Matter, Says County Official

SINCE 2002, Broward County's Web site has included instructions on how to request the removal of protected personal information from documents posted online, said Sue Baldwin, director of the Broward County Records Division.

She added that the Florida county has made the redaction-request instructions more visible on the site in response to the concerns about the disclosure of personal data raised last month by resident and IT professional Bruce Hogman.

For now, according to Baldwin, that is all she is empowered to do under Florida's laws. "Aside from making the redaction-request process as user-friendly and speedy as possible, I do not have the independent authority to take any additional action regarding removing material from the public records," she said.

Baldwin said that citizens who are concerned about their personal data being posted online should check to see if sensitive information is publicly accessible and then ask that it be blacked out.

"People have to assume some responsibility," she said. "At least now, people can look at this stuff and say, 'I don't want people looking at this,' and ask [us] to take it off. They should regard this as an opportunity."

Hogman, who wants online records containing sensitive data taken down until a full solution is found, said he has tried to contact both of Florida's U.S. senators and some state legislators, plus the FBI and the Federal Trade Commission. As of last week, Baldwin was the only person he had heard back from.

"In my estimation, 'do nothing' is not a good solution because it leaves the information out there for public viewing," Hogman said.

– JAIKUMAR VIJAYAN AND KEN MINGIS

BRIEFS

Oracle Buys Billing Software Vendor

Oracle Corp. last week agreed to buy Portal Software Inc., a maker of billing and revenue management software for the communications industry, for about $220 million. Oracle expects the transaction to close in June and plans to integrate Portal's software capabilities into its ERP applications and the CRM software it acquired with Siebel Systems Inc. Oracle said it may use Portal's software for other industries.

Sun Adds Microsoft Link to Thin Clients

Sun Microsystems Inc. has rolled out the second generation of its Sun Ray thin-client devices and software with added links to Windows environments. The new offerings also include smart-card slots to enable "hot desking," which allows the use of Java-based cards to switch devices on the fly, starting up sessions where they left off.

NetApp to Expand Indian Operations

Network Appliance Inc. plans to expand a development center in Bangalore, India, that builds and supports several product lines, including its NetCache product. The center is also likely to run the company's worldwide information systems. The expansion will include a new 180,000-square-foot facility that will house about 750 engineers over the next two years.

IBM Builds Chip Encryption Tool

IBM researchers have developed encryption technology that can be built directly into a microprocessor to help lock down data in mobile phones, PDAs, digital media players and other devices. The technology, called Secure Blue, can be used in consumer electronics, medical and government applications, and digital media. IBM is building the technology into its Power processor. The technology will also work in other vendors' processors.

Continued from page 10

Personal Data

per form as specious.

"The simple truth is these records were safe in the courthouse for 160 years," Bloys said. Now all it takes is Internet access and a rudimentary idea of how to look for sensitive data to find all sorts of information, he added.

Ostergren claimed that simply by "messing around" on county Web sites over the past three and a half years, she has found hundreds of thousands of pages containing sensitive information. She has printed out more than 17,000 records containing people's Social Security numbers, the maiden names of their mothers (often used to verify identities) and the names of minors.

Among the countless nuggets that Bloys said he has found online was the complete medical history of a terminally ill government official in the Texas county of Fort Bend.

Buying Data in Bulk

It isn't always necessary to search through Web sites, because online records can often be purchased in bulk for a fraction of what it would cost to buy them at a courthouse, Bloys said. For example, he said, officials in Fort Bend County last year sold a Florida company online copies of every document ever filed with the county clerk's office. The cost for the estimated 20 million documents was about $2,500, said Bloys, who wrote an article about the transaction in his newsletter.

A call seeking comment on the matter from the Fort Bend County recorder's office hadn't been returned as of *Computerworld*'s publication deadline.

The company that bought the information is among a large number of businesses — including some in India, China and the Philippines — that routinely download records directly from county Web sites, Bloys claimed.

Bruce Hogman, a Broward County county resident who recently raised concerns about the posting of personally identifiable information with Baldwin's office, said real estate professionals and other business users don't need all of the information included in documents posted online.

For real estate transactions, Hogman said, "they need nothing more than the names of the parties, the date of the transaction, the consideration, the book and page in which the data is recorded, together with the legal description — and not the actual image of the documents themselves."

Ostergren said efforts to stop Virginia's Hanover County, where she lives, from posting images of public records online have succeeded so far. But 14 of the state's 121 cities and counties do make records available online, she said, adding that the same thing is being done by counties in states such as Pennsylvania, North and South Carolina, Ohio, Georgia, Arizona, Texas and New York. That includes all five boroughs in New York City, according to Ostergren.

Fogelsong noted that Orange County residents who want information removed from documents can request that it be redacted (see related story, below). "I would love if people would check their records on their own" to ensure that no private data is publicly disclosed, she said.

But Ostergren dismissed such advice, saying Florida and North Carolina are currently the only states that allow residents to ask for their Social Security numbers to be removed from online records that were already posted.

On the other hand, many states have given county clerks the power to refuse to record new documents containing personally identifiable data, Ostergren said. Overall, though, "this online records mess has been the best-kept secret," she added. "Ninety-nine percent of citizens haven't a clue that the records are online in the first place."

Computerworld's Ken Mingis contributed to this story.

Redaction Tools Hunt For, Hide Personal Information

REDACTION SOFTWARE works in much the same way that antispam tools do – by using algorithms to look for specific phrases or words. But they analyze images, not e-mail.

Some vendors use multiple levels of automatic analysis, while others narrow down the number of documents likely to need redaction and then rely on human intervention to help improve the software's automatic redaction capabilities.

"It's a new technology, but a proven technology," said Paul Miller, president of Aptitude Solutions Inc. in Casselberry, Fla. Miller said Aptitude's eRedact software looks for specific numbers, words or combinations of related words, such as "account number" or "Social Security number."

On big jobs involving millions of document images, several thousand pages are culled and manually analyzed by a worker who can verify that data should be redacted, Miller said. The software then automatically adjusts to redact the remaining records based on the manual choices. It typically costs between $200,000 and $300,000, he said.

ImageTech Systems Inc. in Camp Hill, Pa., has built a plug-in redaction module for Kofax Ascent Capture, a tool from Kofax Image Products Inc. in Irvine, Calif., that finds data in documents and forms.

R.J. Oberman, ImageTech's president, said the plug-in module uses several methods, including on-the-fly input from users, automatic processing of data in standard forms and an intelligent algorithm. The module starts at $5,000, but the total cost can exceed $100,000, Oberman said.

Other redaction vendors include SRS Technologies' Systems Technology Group, Appligent Inc. and Image Architects Inc.

– TODD R. WEISS

Data Removal Is a Private Matter, Says County Official

SINCE 2002, Broward County's Web site has included instructions on how to request the removal of protected personal information from documents posted online, said Sue Baldwin, director of the Broward County Records Division.

She added that the Florida county has made the redaction-request instructions more visible on the site in response to the concerns about the disclosure of personal data raised last month by resident and IT professional Bruce Hogman.

For now, according to Baldwin, that is all she is empowered to do under Florida's laws. "Aside from making the redaction-request process as user-friendly and speedy as possible, I do not have the independent authority to take any additional action regarding removing material from the public records," she said.

Baldwin said that citizens who are concerned about their personal data being posted online should check to see if sensitive information is publicly accessible and then ask that it be blacked out.

"People have to assume some responsibility," she said. "At least now, people can look at this stuff and say, 'I don't want people looking at this,' and ask [us] to take it off. They should regard this as an opportunity."

Hogman, who wants online records containing sensitive data taken down until a full solution is found, said he has tried to contact both of Florida's U.S. senators and some state legislators, plus the FBI and the Federal Trade Commission. As of last week, Baldwin was the only person he had heard back from.

"In my estimation, 'do nothing' is not a good solution because it leaves the information out there for public viewing," Hogman said.

– JAIKUMAR VIJAYAN AND KEN MINGIS

AMD

e power of cool

GLOBAL

An International IT News Digest

China Pledges to Help Fight Software Piracy

WASHINGTON

DURING MEETINGS with U.S. trade representatives here last week, Chinese government officials committed to increasing protections for intellectual property in their country.

China will conduct seven special enforcement operations against intellectual property pirates this year, Vice Premier Wu Yi said at a press conference after talks between members of the U.S.-China Joint Commission on Commerce and Trade. The Chinese government will open infringement-reporting centers in 50 cities, she said.

In addition, Wu said that China will accelerate the transfer of piracy cases from administrative to criminal enforcement bodies. That would address complaints by U.S. software vendors that China doesn't adequately enforce its intellectual property laws.

The talks were held a day after the Chinese government announced that all computers sold in the country must now include a preloaded, licensed operating system.

The Washington-based Business Software Alliance commended the Chinese government's move to mandate preloaded software.

Framingham, Mass.-based market research firm IDC estimates that 90% of the software used in China during 2004 was unlicensed.

■ GRANT GROSS, IDG NEWS SERVICE

Two Chinese Vendors Sign Windows Deals

LOS ANGELES

IN ADVANCE of the Chinese government's mandate regarding the use of licensed operating systems, two computer makers in China promised to distribute only licensed versions of Windows under new agreements with Microsoft Corp.

At a ceremony here on April 7, Microsoft signed deals with Beijing-based Tsinghua Tongfang Co. and Huizhou-based TCL Corp. Wu Yi, the Chinese vice premier, attended the ceremony on her way to Washington for the economic and trade talks.

John Litten, communications manager in Microsoft's reseller division, said the Chinese manufacturers also agreed to help educate end users about the benefits of using licensed software, including the availability of vendor-provided support.

Under its deal, Tsinghua Tongfang has agreed to buy $120 million worth of Windows licenses over three years, according to a statement from Chairman Rong Yong Lin. TCL has agreed to purchase $60 million worth of licenses over the same period, said Yang Weiqiang, a group vice president at that company.

Microsoft signed a similar deal last November with Lenovo Group Ltd.

■ BEN AMES, SUMNER LEMON AND NANCY WEIL, IDG NEWS SERVICE

GLOBAL FACT

Percentage of Europe's online population of 82 million people that used instant messaging applications in February

Taiwan President Blasts Google, Yahoo on China

TAIPEI, TAIWAN

IN A speech commemorating a local human rights activist, Taiwan President Chen Shui-bian accused Yahoo Inc. and Google Inc. of compromising free speech in China to boost their corporate profits.

Chen called on the Chinese government and companies such as Yahoo and Google "to respect democracy and freedom, because it is the correct way to ensure continuous future development." Taiwan's president used an annual ceremony for activist Cheng Nan-jung as a platform for his contention that countries should not compromise free speech or freedom of the press.

Neither Google nor Yahoo responded to requests for comment.

In January, Google launched a censored version of its search engine in China, while Yahoo has faced criticism for providing Chinese police with e-mail messages that helped put a journalist in jail for 10 years.

■ DAN NYSTEDT, IDG NEWS SERVICE

Australian State Signs Health Care IT Pacts

MELBOURNE, AUSTRALIA

THE DEPARTMENT of Human Services in the Australian state of Victoria has awarded health care software vendor Cerner Corp. a contract to implement new clinical applications for all of the state's public-sector health providers.

The contract with North Kansas City, Mo.-based Cerner is part of the agency's HealthSmart program, a four-year initiative valued at $323 million Australian ($236 million U.S.).

HealthSmart contracts have also been awarded to TrakHealth Pty. in Sydney, Australia, for a client management system; iSoft Group PLC in Manchester, England, for an integrated patient records system; and Frontier Software Pty. in Melbourne for a human resources system.

In addition, Oracle Corp. won a contract to provide financial and supply management software to the Victoria Department of Human Services.

All of Victoria's HealthSmart technology is expected to be in place by next year.

■ MICHAEL CRAWFORD, COMPUTERWORLD TODAY

Ethernet Service Links Hong Kong to Beijing

HONG KONG

HUTCHISON GLOBAL Communications (HGC) Holdings Ltd. has launched an Ethernet service that connects Hong Kong with Beijing and China's Guangdong province, in an attempt to meet growing corporate demand for networking connections between Hong Kong and mainland China.

HGC, a unit of Hong Kong-based Hutchison Telecommunications International Ltd., said the need for cross-border networking capabilities has been increasing since China joined the World Trade Organization and signed the Closer Economic Partnership Agreement with Hong Kong. The CEPA is designed to improve economic ties between Hong Kong and the rest of China.

The Ethernet service will be offered through an expanded partnership between HGC and Beijing-based China Telecommunications Corp. HGC said the service eliminates the need for companies to reconfigure their networks or install specialized equipment.

The link also lets users adjust the speed of their network connections from a minimum of 2Mbit/sec. to more than 45Mbit/sec., according to HGC.

■ SUMNER LEMON, IDG NEWS SERVICE

Compiled by Mike Bucken.

Briefly Noted

VeriFone Holdings Inc. has agreed to buy rival point-of-sale terminal maker Lipman Electronic Engineering Ltd. in Rosh Haayin, Israel, for about $793 million in cash and stock. San Jose-based VeriFone said Lipman will help it gain access to more wireless and IP-based payment technologies. VeriFone expects to complete the deal by the end of October.

■ PETER SAYER, IDG NEWS SERVICE

Sony Corp. and Samsung Electronics Co. have agreed to jointly build a $2 billion facility in Tangjeong, South Korea, for manufacturing LCD panels. The deal expands S-LCD Corp., a joint venture between Sony and Samsung that operates an LCD production line.

■ MARTYN WILLIAMS, IDG NEWS SERVICE

Comverse Inc. in Wakefield, Mass., has agreed to acquire Netcentrex SA, a vendor of voice-over-IP software in Paris. Comverse will pay about $184 million, plus another $16 million if Netcentrex meets certain financial performance goals. Netcentrex generated about $50 million in revenue last year, said Comverse, which sells software that supports network-based communication and billing services.

■ GRANT GROSS, IDG NEWS SERVICE

Unilever NV has awarded Accenture Ltd. a seven-year contract to provide application development, implementation and support services to its European operations. The deal expands on an earlier pact under which Hamilton, Bermuda-based Accenture provides consulting and IT services to Rotterdam, Netherlands-based Unilever.

China United Telecommunications Corp., the second-largest mobile network operator in China, has introduced a push e-mail service called RedBerry – a name that echoes Research In Motion Ltd.'s (RIM) popular BlackBerry service. RIM is in talks with China Unicom's main rival, China Mobile Communications Corp., about launching the BlackBerry service in China. RIM officials didn't comment on the brand name chosen by Hong Kong-based China Unicom.

■ SUMNER LEMON, IDG NEWS SERVICE

EMC Extends On-site Services Offerings

BY SHARON FISHER AND SHELLY SOLHEIM

EMC Corp. last week extended its professional services arm with the unveiling of an on-site support program to help IT officials manage large storage environments.

In addition, the company today is set to bring out an entry-level disk backup system designed for small and mid-size businesses, along with updates to the full Clariion Disk Library line.

The EMC Managed Services offering is geared for businesses that require multiyear, on-site management of storage environments with more than 100TB of capacity. Under the program, EMC employees are dedicated to a site and provide support based on service-level agreements.

Thomas Schiller, general manager of IT at Toyota Motorsport GmbH in Cologne, Germany, an early user of the service, said that it has enabled his company to focus IT resources on its core business.

With six to eight EMC workers on-site, Toyota Motorsport, which handles the design, manufacturing and operations for the Toyota Formula 1 program, doesn't "need to have [its] own dedicated resources," Schiller said.

Previously, the company used its own IT staff, along with EMC employees, for short-term engagements, he said. Schiller would not disclose how much EMC is paid for the service.

EMC said American Express Co. has also signed a multiyear contract for the new services.

A spokeswoman for New York-based American Express said the company hopes the program can increase its flexibility and improve its cost structure for data storage.

The new entry-level disk backup system, the Clariion DL210, has a capacity of between 4TB and 24TB.

It's a Small World

"An entry-level box for a smaller enterprise is a very good idea," said John Halamka, CIO at Harvard Medical School and CareGroup Healthcare System in Boston.

Halamka said he's not yet familiar with the new low-end product, but said he expects it to offer the reliability he finds on the high-end EMC backup systems at the medical school.

Meanwhile, The Black & Decker Corp. in Towson, Md., plans to evaluate the new low-end model for its remote sites, said Ian McLeavy, manager of global engineering storage. The company already uses EMC's 700 series of bigh-end Clariion disk backup systems, he said.

EMC will also announce today that the full Clariion line of tape drives will now support the IBM iSeries platform and EMC's NetWorker 7.3 backup and recovery software, which EMC gained in its acquisition of Legato Systems Inc. more than two years ago.

This latest announcement shows that EMC is paying attention to user complaints that the company's various acquisitions have not been well integrated, said John Webster, an analyst at Data Mobility Group LLC in Nashua, N.H. ♦

Solheim is a reporter for the IDG News Service.

New Product

The EMC Clariion DL210 disk-based backup system

- Uses 500GB Serial ATA disk drives
- Has up to 24TB capacity
- Supports IBM iSeries systems
- Supports EMC NetWorker backup and recovery software
- Is priced starting at $50,000
- Is shipping now

TD Ameritrade Encryption Project Is Nearly Complete

CIO says work at TD Waterhouse sites should be finished this month

BY LUCAS MEARIAN

Ameritrade Holding Corp. late last year finished rolling out technology to encrypt corporate data as it moves from servers to backup devices, just before its acquisition of TD Waterhouse Group Inc. closed in January. **Jerry Bartlett**, *CIO of the combined firm, called TD Ameritrade Holding Corp., talked about extending the encryption technology to TD Waterhouse sites and other issues at the recent Storage Networking World conference.*

Have you rolled out the Decru encryption technology throughout the combined company? We completed it in the November and December time frame for the Ameritrade facilities. And we're completing it for the combined TD Ameritrade this month.

Was the process of installing encryption technology difficult? The difficulty was around deciding what we were going to do and how we were going to do it — not around the implementation itself. Once we realized that we needed to execute like it's any other infrastructure project, we assigned a project manager with a plan coordinating our infrastructure teams.

How many Decru encryption appliances have been deployed? About a dozen.

Do you have any concerns about unencrypting data for restoration in the future? Not really. We're comfortable with the backward-compatibility commitments. We would be concerned if the encryption algorithm were changed.

How long did it take to deploy the appliances? It took us to do the legacy Ameritrade less than six months. It took us less than three months to do the TD Waterhouse side.

How much data do you encrypt? In the neighborhood of 30TB per week, including full and incremental backups.

How have the regulators reacted to the decision to encrypt your data? The feedback we've received is that they're thrilled about it. So we're thrilled about that.

What other types of storage challenges is your company facing? It's this whole idea of a formal and automated approach to information life-cycle management. We have very well-understood retention rules, but it's too manual.

As we acquire companies and the obligations of those firms become our obligations — client data, client e-mails — that's probably one of the biggest hurdles we have to address. We're just starting to put together a strategy to address it. I think we have a good approach to rationalizing storage around our applications, which is important.

What is your take on the upcoming Storage Networking Industry Association standard to allow migration of data across tiers of storage? My fundamental view is we are, and ought to be, vendor-agnostic. My team's a big believer in standards — in this case, standard interfaces and the ability for a heterogeneous group of vendors to be able to be utilized across the whole data life cycle, I think, is the right direction.

Does that mean the company, now mostly an EMC shop, will look at technology from other vendors? Right now, we're an EMC shop, so as we do mergers and acquisitions, we stick with EMC. It doesn't mean we won't continue to look at vendors whose offerings become potentially higher in quality, availability and resiliency at competitive cost points. A fundamental tenet is [that] we're vendor-agnostic. ▸

New Processes Speed Chain's Salon Openings

BY HEATHER HAVENSTEIN

Great Clips Inc. is about a year away from wrapping up a four-year effort to overhaul and automate its business processes. Officials say the project is a key reason why the company has already been able to increase new store openings from 200 per year to 300.

The Minneapolis-based chain of 2,500 hair salons completed the first phase of the $1 million project in July 2005 by automating and streamlining what had been a 120-step process for opening a new salon.

This July, Great Clips IT developers will begin work on overhauling the business procedures used by managers to work with franchisees and existing salons. And at the beginning of next year, the company plans to launch the last phase of the project: re-engineering its contract management and communication processes.

The full project is slated to be completed in mid-2007.

"In our previous state, it was hard for management to be able to see the performance of the business processes — to see into it and measure it," said Jim Waldo, vice president of IT at Great Clips. The company decided to automate its processes to give executives the visibility they need to manage them more proactively, he said.

That decision came after an internal analysis in 2003 determined that the company's procedures were preventing it from meeting growth plans.

The internal study found, among other things, that people in various steps in the process — such as internal employees, real estate agents and contract managers — had to spend significant time searching for information before handing it off to the next person in the chain.

Great Clips officials decided to automate its processes using Metastorm Inc.'s eWork business process management (BPM) suite and Interwoven Inc.'s MailSite Document Management suite. Metastorm's BPM suite is designed to support design, integration and deployment of new internal procedures while integrating them into existing applications and systems.

For the first phase of the project, from July 2004 to July 2005, Great Clips developers used the Metastorm tool to automate and streamline the course of action for opening a new salon. Prior to completing the first phase, the 120-step process included eight specialized roles and 50 users.

Automation let Great Clips eliminate 20 of those steps. The most important result, Waldo said, was eliminating the steps that required people to wait for "days up to two weeks for information that was already in the building."

The project required significant effort from Great Clips developers working with the third-party tools, Waldo noted.

For instance, he said, the learning curve for Metastorm tools was steep. To make sure all the developers gained proficiency in the product, the company required that its entire development team first attend training as a group and then immediately begin work on a pilot project with limited scope and integration.

In addition, the developers had to make sure Interwoven's MailSite product — which captures and stores content directly from Microsoft Outlook — was tightly integrated with the desktop information manager.

Dennis Byron, an analyst at IDC in Framingham, Mass., said the ideal application of BPM tools is making communications with internal and external users — such as business partners or suppliers — easier. In addition, he noted that overhauling and automating business processes isn't trivial. ▸

Timeline: A Business Automation Project

FALL 2003: Performed process analysis.

JULY 2004: Began work on automating processes for working with franchisees and existing salons.

2003 2004 2005 2006 2007

JULY 2004–JULY 2005: Automated and scaled back 120-step process for opening new salons.

JANUARY 2007–JUNE 2007: Begin work on automating contract management and communication processes.

TD Ameritrade Encryption Project Is Nearly Complete

CIO says work at TD Waterhouse sites should be finished this month

BY LUCAS MEARIAN

Ameritrade Holding Corp. late last year finished rolling out technology to encrypt corporate data as it moves from servers to backup devices, just before its acquisition of TD Waterhouse Group Inc. closed in January. **Jerry Bartlett,** *CIO of the combined firm, called TD Ameritrade Holding Corp., talked about extending the encryption technology to TD Waterhouse sites and other issues at the recent Storage Networking World conference.*

Have you rolled out the Decru encryption technology throughout the combined company? We completed it in the November and December time frame for the Ameritrade facilities. And we're completing it for the combined TD Ameritrade this month.

Was the process of installing encryption technology difficult? The difficulty was around deciding what we were going to do and how we were going to do it — not around the implementation itself. Once we realized that we needed to execute like it's any other infrastructure project, we assigned a project manager with a plan coordinating our infrastructure teams.

How many Decru encryption appliances have been deployed? About a dozen.

Do you have any concerns about unencrypting data for restoration in the future? Not really. We're comfortable with the backward-compatibility commitments. We would be concerned if the encryption algorithm were changed.

How long did it take to deploy the appliances? It took us to do the legacy Ameritrade less than six months. It took us less than three months to do the TD Waterhouse side.

How much data do you encrypt? In the neighborhood of 30TB per week, including full and incremental backups.

How have the regulators reacted to the decision to encrypt your data? The feedback we've received is that they're thrilled about it. So we're thrilled about that.

What other types of storage challenges is your company facing? It's this whole idea of a formal and automated approach to information life-cycle management. We have very well-understood retention rules, but it's too manual.

As we acquire companies and the obligations of those firms become our obligations — client data, client e-mails — that's probably one of the biggest hurdles we have to address. We're just starting to put together a strategy to address it. I think we have a good approach to rationalizing storage around our applications, which is important.

What is your take on the upcoming Storage Networking Industry Association standard to allow migration of data across tiers of storage? My fundamental view is we are, and ought to be, vendor-agnostic. My team's a big believer in standards — in this case, standard interfaces and the ability for a heterogeneous group of vendors to be able to be utilized across the whole data life cycle, I think, is the right direction.

Does that mean the company, now mostly an EMC shop, will look at technology from other vendors? Right now, we're an EMC shop, so as we do mergers and acquisitions, we stick with EMC. It doesn't mean we won't continue to look at vendors whose offerings become potentially higher in quality, availability and resiliency at competitive cost points. A fundamental tenet is [that] we're vendor-agnostic. ▸

New Processes Speed Chain's Salon Openings

BY HEATHER HAVENSTEIN

Great Clips Inc. is about a year away from wrapping up a four-year effort to overhaul and automate its business processes. Officials say the project is a key reason why the company has already been able to increase new store openings from 200 per year to 300.

The Minneapolis-based chain of 2,500 hair salons completed the first phase of the $1 million project in July 2005 by automating and streamlining what had been a 120-step process for opening a new salon.

This July, Great Clips IT developers will begin work on overhauling the business procedures used by managers to work with franchisees and existing salons. And at the beginning of next year, the company plans to launch the last phase of the project: re-engineering its contract management and communication processes.

The full project is slated to be completed in mid-2007.

"In our previous state, it was hard for management to be able to see the performance of the business processes — to see into it and measure it," said Jim Waldo, vice president of IT at Great Clips. The company decided to automate its processes to give executives the visibility they need to manage them more proactively, he said.

That decision came after an internal analysis in 2003 determined that the company's procedures were preventing it from meeting growth plans.

The internal study found, among other things, that people in various steps in the process — such as internal employees, real estate agents and contract managers — had to spend significant time searching for information before handing it off to the next person in the chain.

Great Clips officials decided to automate its processes using Metastorm Inc.'s eWork business process management (BPM) suite and Interwoven Inc.'s MailSite Document Management suite. Metastorm's BPM suite is designed to support design, integration and deployment of new internal procedures while integrating them into existing applications and systems.

For the first phase of the project, from July 2004 to July 2005, Great Clips developers used the Metastorm tool to automate and streamline the course of action for opening a new salon. Prior to completing the first phase, the 120-step process included eight specialized roles and 50 users.

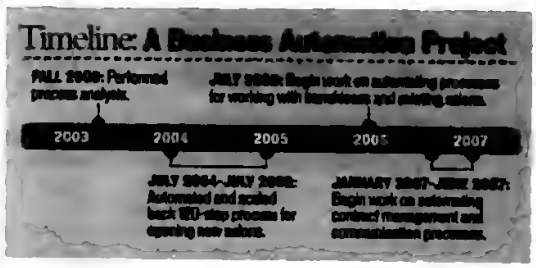
Automation let Great Clips eliminate 20 of those steps. The most important result, Waldo said, was eliminating the steps that required people to wait for "days up to two weeks for information that was already in the building."

The project required significant effort from Great Clips developers working with the third-party tools, Waldo noted.

For instance, he said, the learning curve for Metastorm tools was steep. To make sure all the developers gained proficiency in the product, the company required that its entire development team first attend training as a group and then immediately begin work on a pilot project with limited scope and integration.

In addition, the developers had to make sure Interwoven's MailSite product — which captures and stores content directly from Microsoft Outlook — was tightly integrated with the desktop information manager.

Dennis Byron, an analyst at IDC in Framingham, Mass., said the ideal application of BPM tools is making communications with internal and external users — such as business partners or suppliers — easier. In addition, he noted that overhauling and automating business processes isn't trivial. ▸



The Mandate to Improve IT Service

Releasing a wave of measurable business value

There is a peculiar irony that characterizes IT in organizations today. On the one hand, IT is most definitely at the vanguard of both customer service and service to internal constituents. On the other hand, IT is still looked upon in many companies not as a provider of business value, but as a cost center.

To counter this perception and give IT a seat at the corporate strategy table, leading organizations are discovering there is real and definable business value to improving IT service. By doing so, IT management can define and then efficiently deliver business-critical IT services at their point of maximum effectiveness, supporting business goals and cementing IT's role as an enabler. In other words, improved service is key to unleashing IT's tremendous potential energy and giving a business what it really wants, namely a competitive differentiator and competitive advantage.

Improving service is not simply a cool idea for gaining respect. The real driver is the business environment itself, where the only constant is constant change brought about by forces like regulations, mergers, shifting customer demands, and internal financial requirements. A service-driven IT organization that is process-oriented and focused on business requirements actually leads the business in responding quickly and decisively to these changes and upheavals. That's a far cry from an IT organization regarded as a financial black hole.

How to get there from here

With so much to gain by improving service, a common question for IT managers is, "What's the best approach for doing so?" The answer is for IT to make continuous improvements to service management and service availability.

Service management improvements effectively enable companies to control change and resolve issues using a set of industry best practices based on long-standing IT Infrastructure Library (ITIL) standards. With improved service management, a business can better integrate processes that are far-flung and fragmented, thereby providing far greater visibility into key financial and operational metrics. For business, this is a big win.

For example, CA Service Management from CA provides a business interface to IT services by way of a service catalog to calculate the complete costs of service delivery while assuring that desired service levels can actually be reliably delivered. The service catalog can offer variable costs for different service levels, in terms that line-of-business managers can easily comprehend. This solution can also ensure that required software is deployed in accordance with license requirements.

Improving service availability, meanwhile, optimizes the reliability, performance, and security of the IT environment to deliver services in support of the business with a high level of automation. The best service availability solution is one that can effectively tune the IT infrastructure to keep vital business services online and accurate.

That means finding a solution that monitors and manages all infrastructure components in real time. Moreover, when the solution identifies problems, it has to correct them immediately while learning intuitively from historical problem resolution to then manage more proactively in the future. These are the tenets upon which CA built its CA Service Availability solution, which also maps IT components to the business services they support.

Big benefits from improving service

Concerted efforts to boost IT service have been shown to pay handsome dividends. By one estimate, companies with best practices in place for a streamlined, well-managed environment can reduce total cost of IT ownership by nearly one-third.

Beyond gaining pure efficiencies, companies that invest in solutions to improve services gain previously hidden insights into applications, systems, and networks, which in turn become far more proactive to change in anticipation of problems. So systems are not merely available, but they are also finely tuned to deliver consistently high-quality information on demand.

Improving services can markedly increase the ability of a business to respond to ever-present change, much of which is unforeseen. When IT can respond quickly to such change, the rest of the business is encouraged to pursue continuous, incremental process improvement. And this leads to the business holy grail of lower costs, faster cycle time, and superior bottom-line results.

CHANGE = STABILITY

If there's one constant in business today, it's change. But large or small, internal or external, change doesn't have to impede IT service delivery. Think of change as an opportunity for IT to satisfy fluctuating demand while maintaining a stable, productive work environment. With integrated CA software solutions for service management and service availability, you can unify and simplify the way you manage complex IT services across the enterprise. Anticipate and prioritize shifting demand. Automate processes to ensure timely delivery and reliability of service. And leverage industry best practices such as ITIL. It's all possible with our unique approach to managing technology called Enterprise IT Management (EITM). To learn more about how CA solutions can stabilize change to create a true service-driven IT environment, visit **ca.com/deliver**.

ca

Misuse of Insurer's Data Points to Inside Threats

Users cite need for tools that can help monitor traffic on corporate networks

BY JAIKUMAR VIJAYAN

AN INCIDENT in which an employee at Progressive Casualty Insurance Co. wrongfully accessed information about foreclosure properties she was interested in buying highlights the IT security dangers posed by corporate insiders — and the need for tools that can help guard against misuse of data.

Progressive officials confirmed this month that the Mayfield Village, Ohio-based company notified 13 people in January that personal information — including their names, Social Security numbers, birth dates and property addresses — had been accessed by an unauthorized employee who has since been fired.

Michael O'Connor, a spokesman for Progressive, said the company was alerted to the situation when a woman in Ohio complained about receiving calls from an agent inquiring about her house being under foreclosure. The employee "wrongly used the information in a real estate database," O'Connor said. He noted that although no hacking was done to get at the data, the agent's actions constituted a violation of Progressive's code of ethics.

"We investigated the situation, the employee was terminated, and we alerted the people whose data was accessed," he said, adding that the matter was resolved in January.

Malice and Accident

Such incidents underscore the threats posed to corporate data by malicious insiders and by workers who accidentally leak sensitive information, said Phil Neray, a vice president at database security tools vendor Guardium Inc.

"Most companies have done a good job with perimeter security," Neray said. But now there's a growing need for tools that can help users monitor and audit all activity inside their networks, databases and applications, he added.

For instance, Sirva Inc., a Westmont, Ill.-based provider of relocation services, is using an appliance from Mountain View, Calif.-based Reconnex Corp. to help keep tabs on its intellectual property and other sensitive data while it goes through a series of divestitures.

"One of the things that happens after a divestiture is that people take the stuff they are working on to their new companies," said Chuck Shmayel, vice president of infrastructure and security at Sirva.

The Reconnex appliance sits at the network-egress poiots in each of Sirva's four data centers and monitors traffic to ensure that confidential information doesn't exit the company's networks, either by accident or design.

It isn't just Sirva's own data that is at stake. "As a relocation service, we handle a lot of confidential information on behalf of our customers, and we want to make sure it's protected," Shmayel said.

Monitoring the data that is flowing out of networks can go a long way toward mitigating accidental as well as deliberate leaks, said Mark Moroses, senior director of technical services at Maimonides Medical Center in Brooklyn, N.Y.

Under the Health Insurance Portability and Accountability Act, Maimonides is required to have controls for securing protected health information. The hospital is using Reconnex's appliance to detect if such data is leaving its networks in an unauthorized way.

> **"A patient is not going to come to our hospital if they think we are not doing everything to protect their information."**
>
> MARK MOROSES, SENIOR DIRECTOR OF TECHNICAL SERVICES, MAIMONIDES MEDICAL CENTER

"A patient is not going to come to our hospital if they think we are not doing everything to protect their information," Moroses said.

Microsoft Finally Issues Patch for Exploited Browser Bug

Vendor says that monthly schedule avoids disruption

BY ROBERT McMILLAN

Microsoft Corp. last week released its security software patches for April, including one to address an unpatched bug in the Internet Explorer browser that hackers had been exploiting for several weeks.

As expected, the company released five patches addressing critical vulnerabilities in IE and the Windows operating system. Microsoft also released fixes for Outlook Express, Windows FrontPage Server Extensions and SharePoint Team Services 2002.

The list of patches for IE includes a fix for the vulnerability that hackers had exploited by tricking users into visiting sites that took advantage of the bug and then conning them into downloading unauthorized software on their PCs.

The problem was serious enough that security vendors eEye Digital Security in Aliso Viejo, Calif., and Determina Inc. in Redwood City, Calif., created patches to address it. Last week, eEye reported more than 156,000 downloads of its software.

Isabel Maldonado, a LAN administrator in the attorney's office of Maricopa County, Ariz., followed Microsoft's advice to IE users to avoid hackers by disabling Active Scripting on the 1,100 workstations she administers.

After disabling the software, Maldonado said her Phoenix-based staff fielded about 100 support calls over a two-week period.

Microsoft has said that it tends to avoid releasing early patches — even when they relate to bugs that hackers are already exploiting — because customers find the regular monthly patch releases far less disruptive.

But Maldonado said she would have been happy to have the IE problem patched earlier. "I would have much rather they'd rushed out a patch," she said. "I can't think of a customer that would say, 'Oh no, don't send me the patch right now,' if there's a zero-day alert."

Though he does not expect a major malware outbreak following the release of the patches, Jonathan Bitle, a product manager at security software vendor Qualys Inc. in Redwood Shores, Calif., said that hackers are likely to take advantage of some of the new vulnerabilities.

"With so many issues addressed by these patches . . . we expect that we might see some aftershocks," he said. "These issues could easily be exploited leveraging the naivete of inexperienced users."

Microsoft also released patches for a similarly critical vulnerability in the way Windows Explorer handles Component Object Model objects and for a vulnerability in an ActiveX control called RDS.Dataspace, which is distributed with the Microsoft Data Access Components.

McMillan writes for the IDG News Service.

Oracle Posts Exploit Code for Database Flaw

ORACLE CORP. appears to have accidentally released details about an unpatched security vulnerability in its database software, including sample code for exploiting the flaw.

The information about the vulnerability was included in a note that was briefly posted on Oracle's MetaLink customer support portal on April 6.

Oracle removed the information the next day after being informed of the security risks, said Alexander Kornbrust, a business director at Red-Database-Security GmbH in Neunkirchen, Germany.

Kornbrust distributed an advisory about the vulnerability to the Full Disclosure security mailing list last Monday. The security researcher said he decided to go public with the information about the vulnerability because enough people had already seen Oracle's MetaLink note to pose a risk for users of the database.

An Oracle spokeswoman declined to comment about how the exploit code was released. She said the company plans to provide a software fix for the database hole "in a future quarterly patch update," although it won't be in the next set of security patches that Oracle plans to release tomorrow.

To exploit the vulnerability, an attacker would first need to have a user account on an Oracle database. By creating specially crafted queries, users who normally would only be able to read data could change the underlying information in a database.

—ROBERT McMILLAN, IDG NEWS SERVICE

Sybase Updates SQL Anywhere Database

BY ERIC LAI

The iAnywhere Solutions Inc. unit of Sybase Inc. today starts shipping a beta release of Version 10 of its SQL Anywhere embeddable database, which promises improved performance and new backup features.

The SQL Anywhere beta comes nearly three years after SQL Anywhere 9 became available, said Breck Carter, a database consultant at RisingRoad Professional Services in Toronto and author of a SQL Anywhere manual.

The typical gap between releases of the database has been 18 months, he said.

Uno Money Transfers runs SQL Anywhere as its corporate database on Microsoft Corp.'s Windows Server 2003 operating system. SQL Anywhere manages the Miami-based financial services firm's 40GB database, which handles all of its international money transfers, according to Luiz Paulo, vice president of technology at the company.

Paulo said he plans to upgrade to the new version to use its new data-mirroring capabilities for safe backups and for its intraquery parallel-computing feature, which will speed transactions on Uno's four-way Xeon server.

New Features

The new version of the database also adds encryption capabilities, support for materialized views for faster access, new performance-analysis tools for developers and the ability to split up large queries among multiple processors, said Chris Kleiseth, iAnywhere's senior director of engineering.

Version 10 also adds integration with Microsoft's Visual Studio .Net 2.0 environment and support for the Symbian operating system, Kleiseth said.

SQL Anywhere has so far been deployed 10 million times, according to Dublin, Calif.-based Sybase.

Intuit Inc., which embeds SQL Anywhere 8 in its QuickBooks 2006 accounting software, expects to use the revised database in a future version of its software, said Tim Child, director of engineering at Intuit.

Child said he is impressed with Version 10's database-encryption feature and its snapshot-isolation feature, which he says allows for high-speed reporting.

The beta of SQL Anywhere 10 runs on Windows and Linux. Sybase plans to ship a final version for those two operating systems in the third quarter. Final versions for Solaris and the Macintosh will ship in the following quarter, said Kleiseth.

Debate Over Costs, Benefits Of Certification Is Unsettled

Initials can provide opportunity, more pay but can't guarantee competence

BY LAMONT WOOD

IT'S NOT hard to write the initials after the name of a networking professional: CCIE for Cisco Certified Internetwork Expert, or CNE for Certified Novell Engineer, among dozens of others.

The initials mean that someone is a certified professional for a specific task or product. But before going through the process of earning such a certification, a networking professional should determine whether those initials are worth the effort necessary to acquire them.

"It's a tough question," said Robert Rosen, president of Share, the IBM mainframe user group, and CIO of the National Institute of Arthritis and Musculoskeletal and Skin Diseases in Bethesda, Md. "But I know a lot of people who use them as a gating factor [when hiring], so if you want to maximize your opportunities, they're a good thing to have."

"It certainly is worthwhile," said Matthew Cody, a convergence engineer at Verizon Communications Inc.'s offices in Maplewood, N.J.

Four years ago, Cody began a quest to acquire four different Cisco Systems Inc. certifications to gain specialized skills. The effort eventually led to a new job with a 10% pay increase, he said.

The downside of certification, Rosen said, is that it doesn't guarantee competence.

"I have seen people with great paper certifications who could not troubleshoot their way out of a paper bag," Rosen said. "Some are great test-takers, but they can't apply it. The certificate shows they have made some effort to learn the technology, but the key to hiring is what they have done with it. Can they address real-world problems?"

Bureaucrats love certificates, Rosen said, because it gives them a box to check off, "but that's not doing due diligence. You have to ask things like, 'Tell me about a really interesting problem you solved and how you solved it.'"

"It would be foolish to hire someone just based on certification, since you also have to make sure they know what they are doing," Cody noted. "It's possible to have a good career without certifications, but certifications make it easier to get in the door."

David Foote, president of Foote Partners LLC, a human resources research firm in New Canaan, Conn., said his latest IT compensation survey, released last month, found that networking certification resulted in an average pay premium of 9.1% in the first quarter of 2006. The average premium for all certifications is 8.2%.

Certifications can offer benefits to organizations as well as individuals, added Cushing Anderson, an analyst at IDC.

IDC surveys have found that, compared with a having a staff that has no formal training, having a staff that holds certifications should increase an organization's ability to resolve networking failures by 20% to 40% and reduce the number of unexpected outages by 10%, Anderson said.

Also, "people see [the offering of certification classes by employers] as a benefit and are more loyal," he noted.

Anderson did note that the certification process can be time-consuming and costly.

Classroom training programs can take 10 to 12 days at a cost of $500 to $1,000 per day and are often funded by the student's employer, he said. Online and self-directed study through books and videos are less-expensive alternatives.

Cody recalled that each of his four certifications required passing four or five exams. He kept the total cost of each certification to about $125 by using self-study methods and online training programs. Cody estimated that classroom training for each exam would have cost about $3,000 in metropolitan New York.

> "I have seen people with great paper certifications who could not troubleshoot their way out of a paper bag. Some are great test-takers, but they can't apply it."
>
> ROBERT ROSEN, PRESIDENT, SHARE

Of course, there are certifications, and then there are certifications, noted Neill Hopkins, vice president of skills development at The Computing Technology Industry Association Inc. in Oakbrook Terrace, Ill.

Hopkins divided the field into high- and low-stakes certificates. High-stakes certificates, which offer the most benefit, involve taking carefully developed tests delivered in a proctored setting. Low-stakes tests may be administered online with no precaution against cheating or imposters.

Nonetheless, Hopkins said, low-stakes testing can be beneficial for self-assessment.

Wood is a freelance writer in San Antonio.

Texas Seeks Help in Consolidating Data Centers

One of several efforts by states to cut IT costs

BY PATRICK THIBODEAU

The state of Texas is seeking proposals from outsourcers to consolidate 31 data centers that run 16 mainframes and 7,000 servers and employ more than 500 people. The move is part of an effort to cut costs and eliminate duplication.

Earlier this month, Texas issued a request for proposals, which are due by the end of May. The state plans to select a vendor for the project by year's end, said Leslie Mueller, assistant director for customer services at the Texas Department of Information Resources in Austin.

The state's IT oversight agency believes that Texas "can get tremendous value" from such a project by eliminating duplications in its infrastructure, said Mueller. Analysis determined that annual data-center operating costs in Texas total about $107 million.

The state legislature mandated the consolidation in a measure approved last summer. The agency hasn't yet decided how many data centers will remain after the consolidation is completed.

Consolidation Trend

Texas is hardly alone among state governments in planning a consolidation project, but its initiative is one of the largest.

For example, a survey of 34 states, including Maryland, Massachusetts and New Jersey, by the National Association of State Chief Information Officers (NASCIO), shows a solid push at the state level toward data-center consolidation.

The survey also found that many states are considering moving to shared-services delivery in an effort to cut costs. Several states are looking to companies to provide data-center operations, communications systems, payment systems and disaster recovery as services, the NASCIO survey found.

According to the NASCIO report, about 77% of the state officials surveyed said that they had either consolidated data centers or have projects in progress. In addition, nearly 85% of respondents reported shared data-center services projects under way.

The consolidation efforts and the use of and demand for shared services "were higher than I expected them to be," said John Gillispie, who is chief operating officer at the Iowa Department of Administrative Services' Information Technology Enterprise. He is also co-chair of the NASCIO committee that conducted the survey and reported some of the findings. "I think everybody is seeking efficiency," Gillispie said.

There are several factors driving the consolidation and shared-services efforts by the states, including aging IT workforces, legacy systems and the advent of technologies that many staffs aren't prepared for, said John Lovelock, an analyst at Gartner Inc.

The Stamford, Conn.-based research firm predicts that by 2010, at least half of all state governments will investigate outsourcing initiatives to support major operations.

Lovelock called the use of shared services "an enabling step" that moves a state closer to outsourcing, because it's "taking responsibility a half a step away" from the state agency that uses the service.

The data-center consolidation in Texas, for instance, is seen as a step toward improving interoperability between various agencies, setting the stage for the use of shared services.

SAN Helps Chemical Firm Keep Oil Wells Pumping

Benchmark Energy taps iSCSI system

BY SHARON FISHER

Everyone knows you can't do a good frac job without slurry.

And nobody knows this better than Steve Collins, manager of IT services at Benchmark Energy Products LP, a supplier of chemicals to the oil industry.

It's his job to give Benchmark workers and clients the computer resources needed to make sure that the slurry — a gel that turns into an oatmeal-like sludge — is available for "frac jobs," where the gel is pumped into an oil well under high pressure to fracture the ground to make the oil flow better.

Benchmark installed a $60,000 storage-area network (SAN) from EqualLogic Inc. in Nashua, N.H., about a year ago to improve its disaster recovery and backup capabilities. The SAN replicates Benchmark's BizNet accounting software and Microsoft Exchange e-mail data.

Collins said the accounting system gets replicated every night from Benchmark Energy's Houston headquarters to its largest facility, in Midland, Texas, over the SAN's 3Mbit/sec. point-to-point connection.

The SAN provides 3TB of storage and supports 130 people across three sites. "The SAN has given me better control of our volumes and data," Collins said.

He said the bulk of the accounting and e-mail data was moved onto the SAN within two weeks of starting the project. Now the company is migrating data being created as it upgrades the BizNet software to work with Microsoft's SharePoint collaboration software and Access database.

Benchmark last week moved to unify its backups by buying a Dell Inc. LTO-3 autoloader, based on the linear-tape open standard, that is consistent with the SAN. It performs tape backups using EMC Corp.'s Retrospect software.

Benchmark's clients include oil industry giants such as Halliburton Co. and Schlumberger Ltd. "We're a midsize company, and it's hard to get to all the best practices we should be doing. We need a lot of bang for the buck because we're not able to throw a lot of people at a project."

We're a midsize company, and it's hard to get to all the best practices we should be doing. We need a lot of bang for the buck because we're not able to throw a lot of people at a project.

The SAN has become a key tool for meeting those requirements, he said.

Collins began evaluating backup and disaster recovery technologies more than a year ago, first an iSCSI SAN system from EqualLogic and then Fibre Channel and iSCSI technologies from EMC.

Collins said he was impressed with the ease of use of EqualLogic's SAN technology. "I was already pretty much sold on iSCSI," he said. "I always had a knock against Fibre Channel. It's not known for how easy it is to use."

As for EMC, Collins said, "they were pushing Fibre Channel, which was much more expensive." EMC also offered an iSCSI SAN, but Benchmark went with EqualLogic instead.

Roger Cox, an analyst at Gartner Inc. in Stamford, Conn., said that while EMC offers similar iSCSI SAN products, he believes that EqualLogic's is easier to use.

DON TENNANT

A Documented 'Uh-oh'

WHEN *Computerworld*'s Jaikumar Vijayan broke the story last week about a Florida county that posts on its Web site documents with residents' personal information, we knew we'd snagged a big one. But it wasn't until Vijayan's pursuit of the story uncovered the extent to which the practice is carried out all over the country that we understood what we were on to. It was then that an expletive or two echoed through the newsroom. Rough translation: "Uh-oh."

It began, as many of our stories do, with a tip from a reader. Bruce Hogman, a resident of Broward County, Fla., with 30 years of IT experience, wanted us to be aware that the county's Web site is a treasure trove of personal information — including Social Security, bank account and driver's license numbers — contained in property records and other public documents. According to Hogman, Florida's two senators, various state legislators, the FBI and the Federal Trade Commission had all turned a deaf ear to his concerns about these online records being used to aid identity theft and other forms of fraud.

In all fairness, it's not surprising that these government officials might dismiss Hogman as a crackpot. If his concerns were legitimate, why hadn't they been raised sooner? Why hadn't there been a huge clamor about a practice that, if true, would be so blatantly ill-conceived and contrary to the public good?

Yet if the officials had bothered to investigate Hogman's claims, they would have found that everything he said is true. If any one of them had phoned Sue Baldwin, director of the Broward County Records Division, Baldwin could have confirmed it as casually and as matter-of-factly as she did with Vijayan.

"All this information has been out there and available since the beginning of time," she told Vijayan last week. "It was out there, and the people who were educated about it knew it was there. It's been online since 1999." Moreover, the same situation exists in "all the counties in Florida [and] lots of [other] states," Baldwin said.

Now that Vijayan's reporting, which substantiated those comments, has been picked up by several other national media outlets and we've been educated about what can only be characterized as an outrageous, far-reaching breach of personal privacy and security, it will be interesting to see what happens next.

State and county governments will likely downplay the issue, arguing that many documents by statute are available for public reference in county offices, and that going the online route saves time and resources. Clearly, making images of these documents available online was done with the best of intentions, but the practice was horribly shortsighted. Now we have millions of document images posted online, and the process of expunging (typically called "redacting" in document-imaging circles) sensitive information such as Social Security numbers is a time-consuming, expensive process.

It's difficult not to feel some compassion for cash-strapped state and county governments that face a problem that's so immediate and so overwhelming in its scope. But denying or downplaying the severity of the threat is unfair to the millions of people whose privacy and security are potentially at stake. And equating the availability of documents online with their availability in a locked county courthouse is irresponsible.

"Uh-oh" is right. This is bad. And nothing short of immediate, resolute action to make it better is acceptable.

Don Tennant

THORNTON A. MAY

Leadership Is Needed to Handle Data

A GOOD FRIEND who occupies a major position in a prominent global financial services firm is very concerned about the state of leadership in matters involving the management of personal information. To make this point come alive, my friend recently challenged a group of alpha executives attending a Value Studio at the IT Leadership Academy to explain what they would do in the following hypothetical situation:

A person signs up for a subscription to a newspaper's online service. The newspaper company, in the normal course of setting up the account, collects and stores information about the customer, including name, address and credit card number.

Then, in the normal course of providing its service, the newspaper company tracks which articles the customer reads and which advertising links she clicks on. After some time, the customer decides to cancel the service. This is no big deal; it happens all the time. However, not only does she want to stop using the service, she also wants her data back. In fact, she wants the data expunged — not merely deleted, but *really* gone.

Such requests to leave no digital trace aren't common — yet. They will be the norm in the future.

Having set up this scenario, my friend asked the Value Studio participants to assume roles representing four constituencies: IT, marketing, legal and corporate affairs. Faculty members of the IT Leadership Academy played the customer, the CEO of the newspaper company and the newspaper's board of directors.

The groups were given 10 minutes to discuss their strategies, after which they reported their suggested course of action to the CEO.

The legal team, predictably, stuck to the letter of the law. It was their belief that the newspaper need not take any action, since the contract gives the customer no rights to her data, and no such rights are implied. Their position was that the operative legal contract protects the newspaper company from such requests. Three cheers for the legal team for such a textbook display of thinking inside the box.

Neither the corporate affairs team nor the marketing team was happy with the legal team's analysis. The marketing team thickened the plot of this scenario by revealing that this customer is a U.S. senator from the state with the newspaper company's most profitable customer base and that her husband is the founder of a mega-church near the state capital that has more than 1 million members. Both of these teams favored going beyond what was legally required to try to satisfy the ex-customer's request.

As for IT's perspective, the technical team reporting to the CIO wasn't convinced that it could guarantee eradication of any and all traces of the customer, given the disjointed state of the company's customer data systems.

If you were the CIO, what would you suggest? If you were the CEO, what would you want your CIO to tell you? As a citizen in an increasingly information-rich world, what do you think is the right thing to do?

Please send me your response and I will e-mail you the aggregate consensus of the readership.

DAVID MOSCHELLA

IT Spreads, Industry by Industry

WHEN WAS the last time that news from an IT vendor grabbed the attention of the enterprise IT community, let alone the broader business media? If you're like most, you have probably shrugged off Microsoft's Vista delays and the huge proposed mergers that would combine Lucent with Alcatel and AT&T with BellSouth. Compare this reaction with the frothy front-page coverage once given to Windows 95, the browser wars and Linux.

While some may see this relative indifference as the inevitable result of a maturing IT industry, or even as a sign that IT no longer matters, a closer look reveals just the opposite. Enterprise IT has never been more interesting, and technology is now driving business transformation controversies that dwarf the vendor squabbles of the past. Consider the following 10 IT stories that are playing out across much of the developed world.

DAVID MOSCHELLA is global research director at the Leading Edge Forum, a Computer Sciences Corp. company. Contact him at dmoschella@mindspring.com.

1. Governments are debating if and how they should move toward a new generation of identification cards and cross-linked databases. For better or worse, both could be powerful new platforms for societal security and control.

2. The health care industry is struggling to develop the standards and cooperation needed to automate medical records processing. Few paths offer more hope for better care and more effective cost control.

3. The insurance industry is looking at the same sorts of health records and debating whether to use individual information to price insurance coverage based on family history, genetic proclivities, driving habits or other personal traits and behavior.

4. The pharmaceutical industry is considering moving away from its increasingly problematic one-size-fits-all drug manufacturing approach to developing products that are customized to the needs of smaller groups or even individuals.

5. Book publishers and Google are locked in a fierce legal battle to determine what will constitute "fair use" on the Internet. At stake is the scope and manner of future book-content innovation.

6. As services such as iTunes and YouTube take off, the traditional record and television companies are losing their decades-old grip on the identification and promotion of new entertainment talent.

7. Unlike checks, credit cards and ATMs, it looks as if both Internet and mobile phone payment systems will be led not by banks but by new entries, with potentially profound effects on the evolution of the financial services industry.

8. For reasons of cost and reliability, both retailers and manufacturers continue to hold back on massive RFID deployments, with major implications for supply chain advancements.

9. As concerns about global warming increase, various schemes for monitoring and charging for peak-hour driving and other forms of energy use are being either planned or implemented.

10. While the public Internet developed almost accidentally as an open platform not controlled by any one supplier, there is no guarantee that this will always be so. Backbone transmission providers are seeking to expand their influence.

In short, every industry has its own IT-driven story, each of vital interest to its sector. Thus, the real enterprise IT action has moved away from adopting general-purpose products and is now centered on business and industry change. That's the sort of maturity we should all welcome. How is your company's industry changing? And are your IT organization's priorities changing with it?

WANT OUR OPINION?

More columnists and links to archives of previous columns are on our Web site.
www.computerworld.com/columns

READERS' LETTERS

Firefox vs. IE vs. None of the Above

WHY IS IT that most articles regarding browsers are about Firefox and how much better it is than Internet Explorer ["Firefox Finds Cracking the Corporate Market to Be a Challenge," Feb. 13]? While I agree that IE has shortcomings, Firefox isn't much better. It's slow to start, has an unpolished appearance and has limited support for Microsoft technologies like Microsoft Challenge Handshake Authentication Protocol. Why is there never a mention of alternatives like Maxthon and Avant Browser? These browsers, which are more like wrappers for IE that don't use the iexplore.exe executable, offer all the features of Firefox and much more, such as groups, the ability to resume saved sessions, locked tabs, RSS, ad blocking and plug-ins – most without the extra download of extensions or plug-ins.

Charles Haven
IT manager, High Point, N.C.

FIREFOX ISN'T a 100% solution. Because many interactive Web sites, especially those that handle transactions, don't deal with it well, I use IE when doing things like making airline reservations. Nonetheless, Firefox is my browser of choice, and I encourage my more tech-savvy users to use it.

Bill Pratt
Camarillo, Calif.

Security Should Be Easier and Cheaper

THE Q&A with Thomas Noonan, president and CEO of Internet Security Systems Inc. ["New Threats Outflank IT Defenses, Says Vendor Exec," Feb. 27], was filled with such vague, evasive and self-serving answers as to be totally worthless.

I would love for him to explain why deploying a few intrusion-detection devices or enabling global patch management for a network of 7,500 users costs so much, even when the technology is alleged to be highly automated. Vendors claim that they want us to be secure, but their costs for security products and services outside of such highly competitive areas like antivirus and basic anti-spam are priced so as to discourage comprehensive deployment. It isn't surprising that businesses often take a gamble with certain types of threats or ignore certain levels of risk.

In addition, Microsoft, Cisco and other infrastructure vendors are ultimately doing the right thing by adding security functionality. Noonan is clearly concerned about what this will do to demand for his products, but users are tired of bolting security on after the fact.

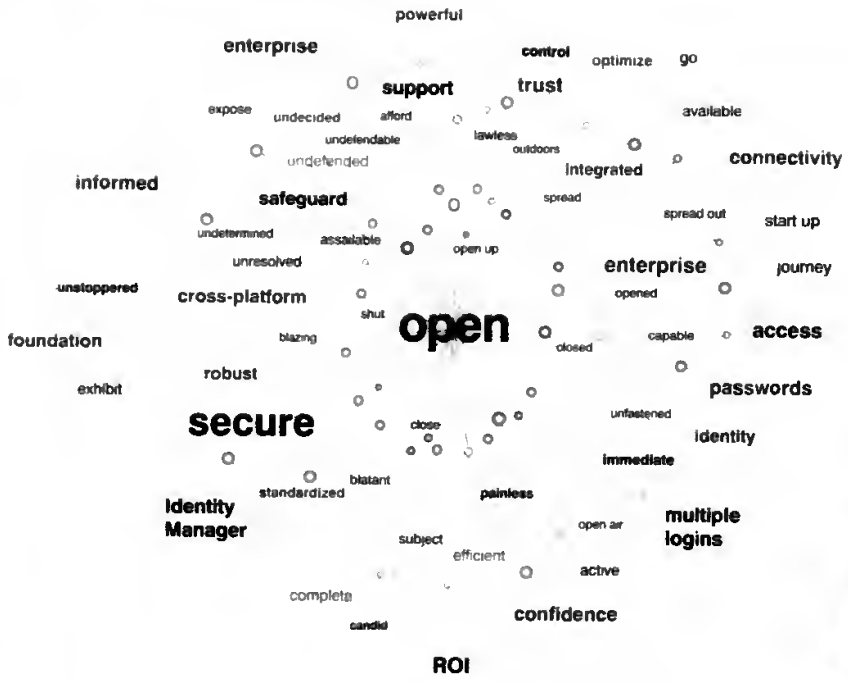
The top five problems with data security, as I see them, are that defense-in-depth strategies are highly desirable yet hideously expensive, many business executives consider the inherent redundancy of defense in depth to be unnecessary; companies are more concerned with avoiding bad publicity than bad security and are willing to gamble on the relationship between the two; we keep trying to make security "seamless," when a greater benefit would be derived from changing user processes; and business executives greet every new security deployment with, "Everything is fixed, right?"

The idea that security is ongoing has yet to be adequately conveyed.

Andrew S. Baker
Director, server operations and security, Caldwell, N.J.

COMPUTERWORLD welcomes comments from its readers. Letters will be edited for brevity and clarity. They should be addressed to Jamie Eckle, letters editor, Computerworld, PO Box 9171, 1 Speen Street, Framingham, Mass. 01701. Fax: (508) 879-4843. E-mail: letters@computerworld.com. Include an address and phone number for immediate verification.

For more letters on these and other topics, go to
www.computerworld.com/letters



DEFINE **YOUR** OPEN ENTERPRISE™

In my Open Enterprise, confidence flows freely because information flows securely.

Every identity, transaction and document represents a possible security risk for your company. A risk that could cost you millions in litigation and overhead associated with data and intellectual capital theft—plus your reputation and brand equity. Security and Identity solutions from Novell®, the most proven in the industry, centralize identity management, reducing the complexity and costs of managing users and access, all while ensuring regulatory compliance for you. There's no better way to secure your enterprise. Or to ensure that your data is working for you and not against you.

Security and Identity solutions from Novell.
This is the way to secure your Open Enterprise.

Novell®

This is Your Open Enterprise.™
www.novell.com/secure

KNOWLEDGE CENTER SECURITY

Risk Formula
The risk-based security model is "forcing us to think more strategically," says Greg Avesian, vice president of enterprise IT security at Textron. PAGE 28

Beyond Posters
You need more than catchy slogans to get workers to take security seriously. Here's how. PAGE 42

No Silver Bullet
Risk is an inherent part of business, says columnist Mark Hall. The biggest security mistake you can make is to take a one-way approach. PAGE 51

EDITOR'S NOTE

WE SECURE information systems because the business would be brought to its knees if we didn't protect trade secrets, vital corporate networks and sensitive data. Yet the business would also be brought to its knees if we spent every last dime in the treasury on security. Yes, it's possible to overspend on security. The trick is to figure out how to reach what ex-CIO Doug Lewis calls "the prudent zone" of security investment.

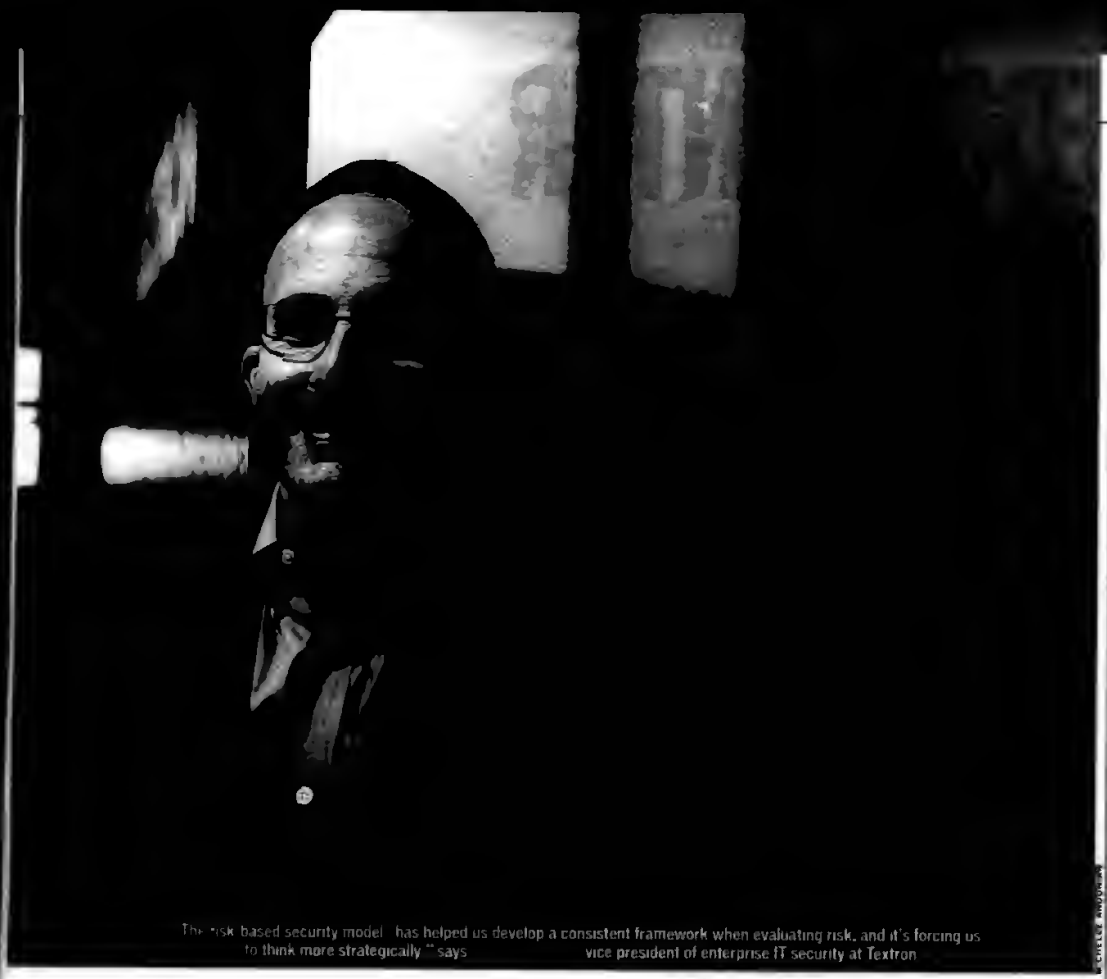
Increasingly, IT leaders are using a risk-based model that directs security spending to the places where a breach would cause the most damage to the business. Companies such as Textron and Standard Chartered Bank are already headed down this road, using metrics to prioritize security risks and allocate resources to mitigate them more efficiently. Some companies use a dashboard to keep an eye on all of those security metrics from a single console. Some classify data at different security levels — much like intelligence agencies do — so they can match the security effort to the classification level.

This new model is replacing "gut feel" decisions with equations like Risk = P x L, where *P* is the probability of an event that will cause a financial loss of *L*. It's a far cry from installing a firewall. But a business-driven, cost-benefit approach to security investments is something the chief financial officer, CEO and board of directors can embrace, which may be the most important benefit of all.

Mitch Betts is executive editor at Computerworld. *Contact him at mitch_betts@computerworld.com.*

The Business Of Security

IT leaders are taking a more businesslike approach to security and risk management.



The risk-based security model has helped us develop a consistent framework when evaluating risk, and it's forcing us to think more strategically," says vice president of enterprise IT security at Textron

The latest approach to security is to put money where damage from a breach would be greatest.

By Steve Ulfelder

Risk Formula

"HOW DO YOU TAKE a risk, have five people take a look at it and have a consistent measure of what it might cost the business?" asks Greg Avesian, vice president of enterprise IT security at Textron Inc. It's not a rhetorical question: The $10 billion conglomerate, based in Providence, R.I., recently embraced the risk-based security model, and quantifying the potential damages of various threats is one of the discipline's major challenges.

In the IT arena, security spending has traditionally been tactical, even scattershot, with a rationale difficult to pin down beyond a vague idea that — to take a cue from Emil Faber, founder of Faber College of *Animal House* fame — Security Is Good. The risk-based security model is an effort to change that.

"Organizations are beginning to deal with risk coherently," says Chris Byrnes, an analyst at Gartner Inc. "Rather than viewing infosec as an island, they're looking across a broader set of risks."

The risk-based model can be a big win for the enterprise because it directs spending where it's needed most, resulting in stronger security. But IT groups are struggling to master the challenges of the still-new concept.

Logical Progression

In the risk-based model, IT and security managers work with business units to identify the biggest threats to the business and then set priorities for security investments. In essence, this model is a cost-benefit analysis to ensure that the security budget is spent wisely.

Clearly, then, the risk-based security model is a logical outcome of the tightening bond between business priorities and technology expenditures. Just as portfolio management and other disciplines tie IT spending to the most productive business initiatives, risk-based security prioritizes spending by the potential damage of various threats.

At Textron, "we looked at [risk-based security] because, like everybody else, we've got a finite amount to spend on risk mitigation," Avesian says. The new model, he adds, "has helped us develop a consistent framework when evaluating risk, and it's forcing us to think more strategically." The company has long emphasized process and views the risk-based model as a complement to its efforts to comply with the Sarbanes-Oxley Act and its devotion to both the Six Sigma quality-control methodology and Control Objectives for Information and Related Technology (Cobit), a set of best practices for IT management.

Sarbanes-Oxley and Cobit each introduced robust controls, Avesian says, while Textron's Six Sigma history taught it to standardize processes wherever possible — which, in turn, entailed measuring progress on that standardization. Indeed, Textron has a resident Six Sigma Black Belt (a rare level of expertise) who is the company's risk-based "process owner."

Analysts and security managers say the growing importance of regulatory compliance has encouraged the adoption of risk-based security. Many demands of Sarbanes-Oxley, the Health Insurance Portability and Accountability Act and other regulations not only help companies become aware of security risks they may have overlooked, but

also dictate controls to plug the holes.

That's what happened at Canadian Pacific Railway Ltd., a multibillion-dollar business with about 8,500 SAP users. In its push to comply with Sarbanes-Oxley (which the company had to follow because it does extensive business with U.S. trading partners), the railway ran Compliance Calculator, a tool from Fremont, Calif.-based Virsa Systems Inc. According to Margaret Sokolov, SAP security and controls lead at Calgary, Alberta-based Canadian Pacific, the compliance software demonstrated that "we had some segregation-of-duties issues" that were problematic for both Sarbanes-Oxley compliance and information security.

The security risks uncovered involved an area in which most businesses underspend: company insiders. Like most large SAP users, Canadian Pacific has a cadre of "superusers" and subject-matter experts who push SAP development forward. These end users had been granted extraordinary access to data and code so that they could tweak interfaces and processes.

When Virsa flagged this access as a barrier to Sarbanes-Oxley compliance, Sokolov's team members realized that a severe threat to data security was right under their noses (although Sokolov hastens to add that the company found no evidence whatsoever of wrongdoing). Prompted by Virsa, the railroad closed the vulnerability with a series of controls. Now, when SAP superusers set out to alter code in an unusual way, a note about the activity is automatically sent to their managers. Afterward, a complete log of the activity is also sent for review and approval.

"This was a case where [compliance software] made us aware that we needed to direct additional spending toward an inside risk," Sokolov says.

IT's Role

Adopting risk-based security is not only inexpensive; properly implemented, it also cuts costs two ways in the long term. First, fewer dollars flow to security efforts in which risks are low. And second, the additional money spent to reduce high-impact risks can save an organization enormous sums by preventing lawsuits, safeguarding proprietary information and, in the case of publicly traded companies, averting negative publicity, which can pummel stock prices.

While risk-based security may remove a certain amount of control from IT's hands, the IT group has a substantial role to play. According to Forrester Research Inc. analyst Michael Rasmussen, understanding and assessing various IT risks "generates a mountain of data that needs to be translated into meaningful information." Forrester suggests that IT groups implement risk dashboards and risk indicators such as intrusion-detection systems to effect this translation.

According to Rasmussen, several vendors are beta-testing risk dashboards, while "some organizations use SMTP applications to develop them internally." A fully operational dashboard, he adds, will include systems monitoring and server status functionality, as well as automated alerts for exceptions. The presentation layer will be customized depending on the end user — a senior business executive may see only a red-light/green-light indicator on his home page, while IT staffers would of course see much more detail.

In the early stages of a shift to risk-based security, IT must also conduct an inventory of all technology assets and then assign a value to each — one of the trickiest phases of the process. This is where ephemeral fears must be turned into hard data. Questions include, "What is the fiscal impact if a given system goes down?" and "What's the fiscal impact if data integrity or confidentiality is compromised?" The answers must address not only short-term transactional problems but also the effects on customer loyalty and stock value.

Gartner's Byrnes says it's vital that business process owners be involved in this stage.

Says Avesian, "I spent six months last year finding a single person in each [of Textron's 20-plus units] to serve as a focal point for security assessments." He has formed a 25-member IT risk management team that meets monthly and is part of Textron's formal governance process.

IT must also play a strong role when controls are being assessed and written. That's hardly new, but in risk-based security, there's a twist.

In the past, once the need for a control was established, IT would simply be sent off to create it, with little attention paid to the price tag. But any control — from an improved firewall to an appropriate-use policy — has an associated cost. Under the risk-based model, these costs must be closely matched to the potential fiscal impact of the risk.

Pinning Down the Numbers

For IT, the challenges of the risk-based security model are as familiar as they are thorny. For starters, the CIO or security officer must establish an ongoing relationship with key business units, for fact-finding and to stay abreast of changing risks. Moreover, the essential need is to quantify that which may resist quantification: assigning a risk factor, and in particular loss estimates, to a new product or partnership is hardly an exact science.

One aspect of the risk-based model may take some getting used to for IT: As information security ceases to be a stand-alone entity and is instead absorbed into the larger risk picture, responsibility for it may be pulled from the technology group. "We believe 30% of [Gartner's] client base has taken infosec away from the CIO," Byrnes says.

Indeed, the most advanced form of risk-based security, dubbed enterprise risk management, is being pushed hard by the large auditing firms. Many businesses that have gone whole-hog into ERM (including virtually all financial services companies, according to Byrnes) have named chief risk officers who report to the CEO or even the board of directors (see "Risk Reducer," page 48).

Tim Maletic, information services security officer at Grand Rapids, Mich.-based Priority Health, is part of a team mulling a move to risk-based security. But he remains unconvinced of the feasibility of assigning an accurate cost figure to various threats. "In a general way, spending your [security] dollars where you can get the most protection is just sensible," he says. "And that's what we're doing."

As an example, he points to the health care company's recent implementation of Cupertino, Calif.-based ArcSight Inc.'s Enterprise Security Manager application. The ESM package compiles and simplifies reports from firewalls, intrusion-detection systems, and antispyware and antispam software, and thus is "the next logical step," Maletic says.

And even though ArcSight has indeed helped him spend his security budget where it's needed most — especially where staffing is concerned — Maletic is skeptical about a grand concept that claims to quantify all security risks.

He's not the only skeptic. Risk-based security, while an appealing idea, appears to demand a level of governance and cooperation with business units that's rare in the day-to-day roller derby of operational IT.

Ulfelder is a freelance writer in Southboro, Mass. Contact him at steve@ulfelder.com.

In Search of a Methodology

RISK-BASED SECURITY cries out for a standardized approach to risk assessment. To date, the closest thing to a leader in this nascent field is from Carnegie Mellon University's Software Engineering Institute.

Operationally Critical Threat, Asset and Vulnerability Evaluation, or OCTAVE, is a self-directed methodology you can use to determine your risk exposure in the context of business activities and priorities. OCTAVE's creators say the system can be used to accomplish the following:

- Identify information assets, vulnerabilities and threats.
- Protect data both tactically and strategically.
- Set up an internal assessment team.
- Provide the risk assessments demanded by HIPAA, Sarbanes-Oxley and other regulations.

While none of the businesses interviewed for this article use OCTAVE today, all say it's on their radar screens as the top risk-based security methodology. Gartner analyst Chris Byrnes agrees with that assessment. He adds that if OCTAVE has a weak point, it's that "you need an advanced, sophisticated governance model in place to really get the most out of it" – thus, the businesses that need OCTAVE the most may be those that are least able to take advantage of it.

To learn more, visit www.sei.cmu.edu

– STEVE ULFELDER

also dictate controls to plug the holes.

That's what happened at Canadian Pacific Railway Ltd., a multibillion-dollar business with about 8,500 SAP users. In its push to comply with Sarbanes-Oxley (which the company had to follow because it does extensive business with U.S. trading partners), the railway ran Compliance Calculator, a tool from Fremont, Calif.-based Virsa Systems Inc. According to Margaret Sokolov, SAP security and controls lead at Calgary, Alberta-based Canadian Pacific, the compliance software demonstrated that "we had some segregation-of-duties issues" that were problematic for both Sarbanes-Oxley compliance and information security.

The security risks uncovered involved an area in which most businesses underspend: company insiders. Like most large SAP users, Canadian Pacific has a cadre of "superusers" and subject-matter experts who push SAP development forward. These end users had been granted extraordinary access to data and code so that they could tweak interfaces and processes.

When Virsa flagged this access as a barrier to Sarbanes-Oxley compliance, Sokolov's team members realized that a severe threat to data security was right under their noses (although Sokolov hastens to add that the company found no evidence whatsoever of wrongdoing). Prompted by Virsa, the railroad closed the vulnerability with a series of controls. Now, when SAP superusers set out to alter code in an unusual way, a note about the activity is automatically sent to their managers. Afterward, a complete log of the activity is also sent for review and approval.

"This was a case where [compliance software] made us aware that we needed to direct additional spending toward an inside risk," Sokolov says.

IT's Role

Adopting risk-based security is not only inexpensive; properly implemented, it also cuts costs two ways in the long term. First, fewer dollars flow to security efforts in which risks are low. And second, the additional money spent to reduce high-impact risks can save an organization enormous sums by preventing lawsuits, safeguarding proprietary information and, in the case of publicly traded companies, averting negative publicity, which can pummel stock prices.

While risk-based security may remove a certain amount of control from IT's hands, the IT group has a substantial role to play. According to Forrester Research Inc. analyst Michael Rasmussen, understanding and assessing various IT risks "generates a mountain of data that needs to be translated into meaningful information." Forrester suggests that IT groups implement risk dashboards and risk indicators such as intrusion-detection systems to effect this translation.

According to Rasmussen, several vendors are beta-testing risk dashboards, while "some organizations use SMTP applications to develop them internally." A fully operational dashboard, he adds, will include systems monitoring and server status functionality, as well as automated alerts for exceptions. The presentation layer will be customized depending on the end user — a senior business executive may see only a red-light/green-light indicator on his home page, while IT staffers would of course see much more detail.

In the early stages of a shift to risk-based security, IT must also conduct an inventory of all technology assets and then assign a value to each — one of the trickiest phases of the process. This is where ephemeral fears must be turned into hard data. Questions include, "What is the fiscal impact if a given system goes down?" and "What's the fiscal impact if data integrity or confidentiality is compromised?" The answers must address not only short-term transactional problems but also the effects on customer loyalty and stock value.

Gartner's Byrnes says it's vital that business process owners be involved in this stage.

Says Avesian, "I spent six months last year finding a single person in each [of Textron's 20-plus units] to serve as a focal point for security assessments." He has formed a 25-member IT risk management team that meets monthly and is part of Textron's formal governance process.

IT must also play a strong role when controls are being assessed and written. That's hardly new, but in risk-based security, there's a twist.

In the past, once the need for a control was established, IT would simply be sent off to create it, with little attention paid to the price tag. But any control — from an improved firewall to an appropriate-use policy — has an associated cost. Under the risk-based model, these costs must be closely matched to the potential fiscal impact of the risk.

Pinning Down the Numbers

For IT, the challenges of the risk-based security model are as familiar as they are thorny. For starters, the CIO or security officer must establish an ongoing relationship with key business units, for fact-finding and to stay abreast of changing risks. Moreover, the essential need is to quantify that which may resist quantification; assigning a risk factor, and in particular loss estimates, to a new product or partnership is hardly an exact science.

One aspect of the risk-based model may take some getting used to for IT. As information security ceases to be a stand-alone entity and is instead absorbed into the larger risk picture, responsibility for it may be pulled from the technology group. "We believe 50% of [Gartner's] client base has taken infosec away from the CIO," Byrnes says.

Indeed, the most advanced form of risk-based security, dubbed enterprise risk management, is being pushed hard by the large auditing firms. Many businesses that have gone whole-hog into ERM (including virtually all financial services companies, according to Byrnes) have named chief risk officers who report to the CEO or even the board of directors (see "Risk Reducer," page 48).

Tim Maletic, information services security officer at Grand Rapids, Mich.-based Priority Health, is part of a team mulling a move to risk-based security. But he remains unconvinced of the feasibility of assigning an accurate cost figure to various threats. "In a general way, spending your [security] dollars where you can get the most protection is just sensible," he says. "And that's what we're doing."

As an example, he points to the health care company's recent implementation of Cupertino, Calif.-based ArcSight Inc.'s Enterprise Security Manager application. The ESM package compiles and simplifies reports from firewalls, intrusion-detection systems, and antispyware and antispam software, and thus is "the next logical step," Maletic says.

And even though ArcSight has indeed helped him spend his security budget where it's needed most — especially where staffing is concerned — Maletic is skeptical about a grand concept that claims to quantify all security risks.

He's not the only skeptic. Risk-based security, while an appealing idea, appears to demand a level of governance and cooperation with business units that's rare in the day-to-day roller derby of operational IT. ▶

Ulfelder is a freelance writer in Southboro, Mass. Contact him at steve@ulfelder.com.

In Search of a Methodology

RISK-BASED SECURITY cries out for a standardized approach to risk assessment. To date, the closest thing to a leader in this nascent field is from Carnegie Mellon University's Software Engineering Institute.

Operationally Critical Threat, Asset and Vulnerability Evaluation, or OCTAVE, is a self-directed methodology you can use to determine your risk exposure in the context of business activities and priorities. OCTAVE's creators say the system can be used to accomplish the following:

- Identify information assets, vulnerabilities and threats.
- Protect data both tactically and strategically.
- Set up an internal assessment team.
- Provide the risk assessments demanded by HIPAA, Sarbanes-Oxley and other regulations.

While none of the businesses interviewed for this article use OCTAVE today, all say it's on their radar screens as the top risk-based security methodology. Gartner analyst Chris Byrnes agrees with that assessment. He adds that if OCTAVE has a weak point, it's that "you need an advanced, sophisticated governance model in place to really get the most out of it" — thus, the businesses that need OCTAVE the most may be those that are least able to take advantage of it.

To learn more, visit www.sei.cmu.edu.

– STEVE ULFELDER

IBM

_THE INVASION

_DAY 13: These underpowered boxes are killing us. They can't handle the workloads. They can't handle the transactions. They can't handle the growing number of users. And I for sure can't handle the costs.

_I'm putting all this junk out where it belongs and buying some real servers.

_DAY 15: I've taken back control by moving to the IBM System p™ platform. It's number one in over 70 leading benchmarks.[1] Take transaction processing for instance — the System p5 570 processes three times as many transactions per minute as the HP rx8620! And its price/performance is better.[2] It's all I ever wanted in a UNIX® server.

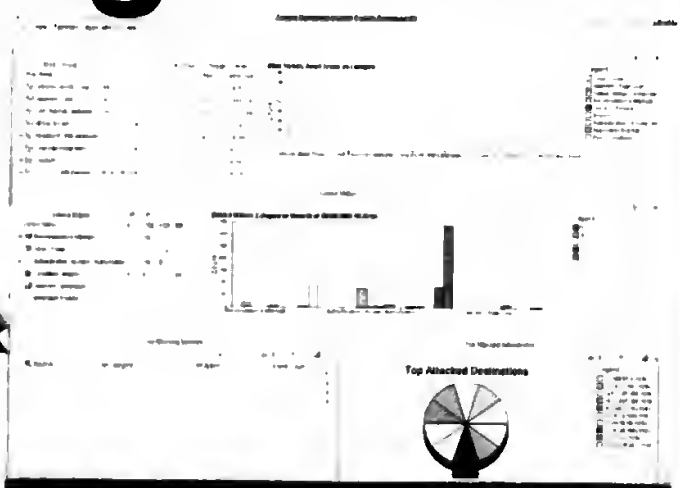
_As for the old servers, well...they kept crashing. Into the ground.

IBM.COM/**TAKEBACKCONTROL**/p5

The Big Picture

Security dashboards offer systemwide visibility from a central console.

By Drew Robb

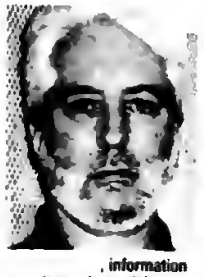


The nFX Open Security Platform from netForensics monitors security events on a single console, allowing Wheaton Franciscan Services to isolate threats earlier.

IT'S USELESS trying to manage a battle when immersed in the fray. So generals have traditionally operated from a hilltop where they have an overview of the conflict below. Effective information security management requires that same type of visibility.

Lee A. Kadel, information security analyst at Wheaton Franciscan Services Inc. (WFS), oversees security at the nonprofit's data center in Glendale, Wis., as well as connections to its 17 hospitals and more than 70 clinics in Colorado, Illinois, Iowa and Wisconsin. He was running nearly 100 security devices, including firewalls, intrusion-protection systems (IPS), virtual private network (VPN) concentrators and authentication servers, but had no way to gain overall insight into the security status of the network.

"We had to manually review the firewalls, manually review the VPN logs and monitor the security logs on the authentication servers," says Kadel. "There were some devices we couldn't manage easily because the volume of event log data was just too great." Like many other security managers, Kadel found that by installing a security information management console, he was able to cut down the monitoring workload and isolate threats earlier, as well as reduce downtime by discovering configuration errors.



, information security analyst at Wheaton Franciscan Services

Limited Dashboards

To bring security and reporting up to the level required for compliance with the Health Insurance Portability and Accountability Act, Kadel installed Edison, N.J.-based netForensics Inc.'s nFX Open Security Platform on five servers in an isolated storage-area network environment. NFX agents receive or collect the data from WFS's security devices. The data is translated into a common database format for storage, analysis and reporting.

"I have a dedicated monitor on my desk, so I can see the state of our network security at any given point in time," Kadel says. "It has given us greater visibility and better reaction time."

Some software vendors sell products called dashboards that are in fact just central management consoles for particular security products. But that doesn't mean that such products aren't helpful.

For example, New York Community Bank uses CA Inc.'s Integrated Threat Management R8. ITM unifies CA's Pest-Patrol Anti-Spyware Corporate Edition and its antivirus software into a single console. The bank uses ITM to centrally manage 3,500 desktops at 170 branches in the greater New York area, as well as its servers. With ITM, help desk staffers can remotely scan the workstations rather than having to travel to a site and do it manually. "Each branch has its own server and PCs," says Assistant Vice President Dan Koppelman. "It has saved us a lot of time and costs, not having to keep IT staff on the road going from PC to PC."

But unlike nFX, such a console can't be considered a true security dashboard.

"This dashboard can be called a vulnerability management dashboard or antivirus dashboard, but not a security dashboard," says Khalid Kark, an analyst at Forrester Research Inc. "A real security dashboard would need to look at security controls in a comprehensive fashion and generate reports on it."

Koppelman has evaluated going to a more complete dashboard but says that what he has now meets his company's needs. But at VeriSign Inc. in Mountain View, Calif., a higher degree of control is needed for protecting the root servers for the .com and .net domains, as well as providing managed security services to thousands of enterprises. VeriSign must protect thousands of production and enterprise servers and hundreds of firewalls and intrusion-detection systems (IDS).

"There were too many places to look for information," says Ken Silva, VeriSign's chief security officer. "The idea is to centralize that into a common console so you really have only one place to look."

VeriSign selected a security management suite from OpenService Inc. in Marlboro, Mass., because of its extensibility. It provided about 80% of the needed functionality out of the box.

"We had the whole system up in about two weeks, and most of that time was spent fine-tuning for the other 20% that it didn't do out of the box," Silva says. "There are some events that we uniquely have at our company that obviously couldn't be preprogrammed into the system."

The system pulls information from the server monitoring service, in-house applications that monitor the domain name service and IDS, IPS, firewall and router logs. All events are sent to a central Unix box that correlates them and synthesizes them into a common event.

Silva reports that network operations center staffers now monitor only a single console instead of a dozen, and they no longer have to dig through several logs to find what is triggering an event. They have been able to reduce mean time to detection by 30% to 50%.

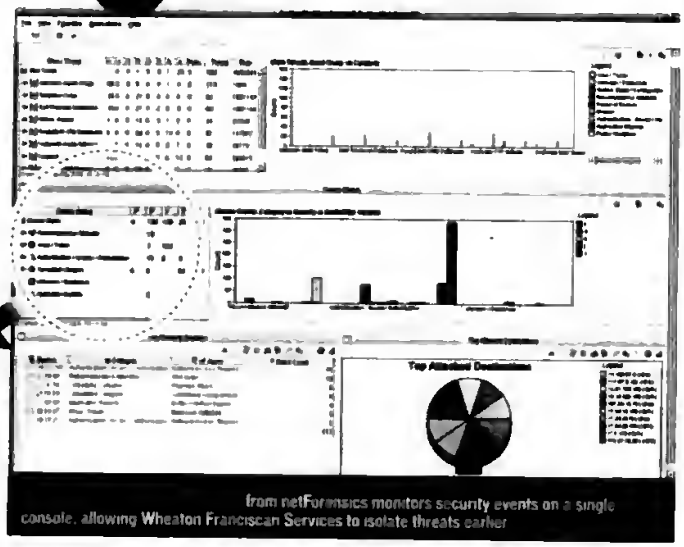
"If done well," says Kark, "a comprehensive security dashboard can not only save a tremendous amount of time and effort for the organization, but also helps security managers get more visibility into their security posture."

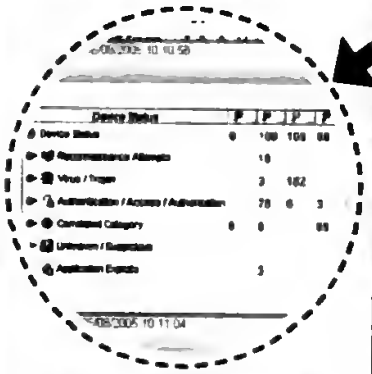
Robb is a Computerworld *contributing writer.*

The Big Picture

Security dashboards offer systemwide visibility from a central console.

By Drew Robb





from netForensics monitors security events on a single console, allowing Wheaton Franciscan Services to isolate threats earlier

IT'S USELESS trying to manage a battle when immersed in the fray. So generals have traditionally operated from a hilltop where they have an overview of the conflict below. Effective information security management requires that same type of visibility.

Lee A. Kadel, information security analyst at Wheaton Franciscan Services Inc. (WFS), oversees security at the nonprofit's data center in Glendale, Wis., as well as connections to its 17 hospitals and more than 70 clinics in Colorado, Illinois, Iowa and Wisconsin. He was running nearly 100 security devices, including firewalls, intrusion-protection systems (IPS), virtual private network (VPN) concentrators and authentication servers, but had no way to gain overall insight into the security status of the network.

"We had to manually review the firewalls, manually review the VPN logs and monitor the security logs on the authentication servers," says Kadel. "There were some devices we couldn't manage easily because the volume of event log data was just too great." Like many other security managers, Kadel found that by installing a security information management console, he was able to cut down the monitoring workload and isolate threats earlier, as well as reduce downtime by discovering configuration errors.

LEE A. KADEL, Information security analyst at Wheaton Franciscan Services

Limited Dashboards

To bring security and reporting up to the level required for compliance with the Health Insurance Portability and Accountability Act, Kadel installed Edison, N.J.-based netForensics Inc.'s nFX Open Security Platform on five servers in an isolated storage-area network environment. NFX agents receive or collect the data from WFS's security devices. The data is translated into a common database format for storage, analysis and reporting.

"I have a dedicated monitor on my desk, so I can see the state of our network security at any given point in time," Kadel says. "It has given us greater visibility and better reaction time."

Some software vendors sell products called dashboards that are in fact just central management consoles for particular security products. But that doesn't mean that such products aren't helpful.

For example, New York Community Bank uses CA Inc.'s Integrated Threat Management R8. ITM unifies CA's PestPatrol Anti-Spyware Corporate Edition and its antivirus software into a single console. The bank uses ITM to centrally manage 3,500 desktops at 170 branches in the greater New York area, as well as its servers. With ITM, help desk staffers can remotely scan the workstations rather than having to travel to a site and do it manually. "Each branch has its own server and PCs," says Assistant Vice President Dan Koppelman. "It has saved us a lot of time and costs, not having to keep IT staff on the road going from PC to PC."

But unlike nFX, such a console can't be considered a true security dashboard.

"This dashboard can be called a vulnerability management dashboard or antivirus dashboard, but not a security dashboard," says Khalid Kark, an analyst at Forrester Research Inc. "A real security dashboard would need to look at security controls in a comprehensive fashion and generate reports on it."

Koppelman has evaluated going to a more complete dashboard but says that what he has now meets his company's needs. But at VeriSign Inc. in Mountain View, Calif., a higher degree of control is needed for protecting the root servers for the .com and .net domains, as well as providing managed security services to thousands of enterprises. VeriSign must protect thousands of production and enterprise servers and hundreds of firewalls and intrusion-detection systems (IDS).

"There were too many places to look for information," says Ken Silva, VeriSign's chief security officer. "The idea is to centralize that into a common console so you really have only one place to look."

VeriSign selected a security management suite from OpenService Inc. in Marlboro, Mass., because of its extensibility. It provided about 80% of the needed functionality out of the box.

"We had the whole system up in about two weeks, and most of that time was spent fine-tuning for the other 20% that it didn't do out of the box," Silva says. "There are some events that we uniquely have at our company that obviously couldn't be preprogrammed into the system."

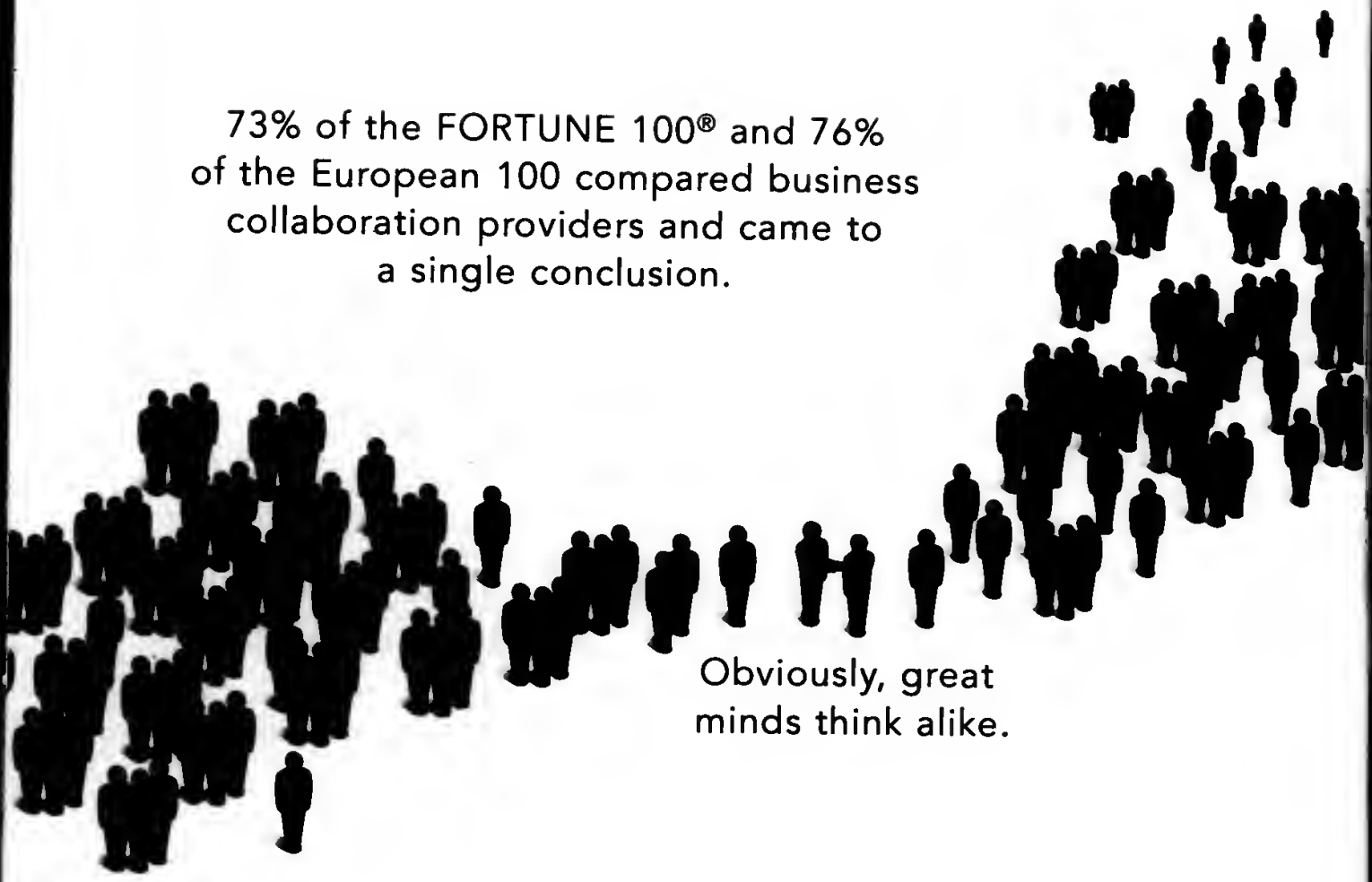
The system pulls information from the server monitoring service, in-house applications that monitor the domain name service and IDS, IPS, firewall and router logs. All events are sent to a central Unix box that correlates them and synthesizes them into a common event.

Silva reports that network operations center staffers now monitor only a single console instead of a dozen, and they no longer have to dig through several logs to find what is triggering an event. They have been able to reduce mean time to detection by 30% to 50%.

"If done well," says Kark, "a comprehensive security dashboard can not only save a tremendous amount of time and effort for the organization, but also helps security managers get more visibility into their security posture."

Robb is a Computerworld contributing writer.

73% of the FORTUNE 100® and 76% of the European 100 compared business collaboration providers and came to a single conclusion.



Obviously, great minds think alike.

Many of the world's most successful organizations rely upon Sterling Commerce to automate their business processes, so they can exchange critical information with their trading partners, subsidiaries and customers. Reliably. Securely. And regardless of the application being used. Sterling Commerce delivers the first platform to meet all the complex challenges of real-world multi-enterprise collaboration. Find out what so many companies already know. Speak to a Sterling Commerce representative today. Or visit **www.sterlingcommerce.com**

BUSINESS APPLICATIONS / BUSINSSS INTSGRATION / BUSINESS INTELLIGENCE / BUSINESS PROCESS MANAGEMENT / SOLUTION DELIVERY

sterling commerce
An AT&T Company

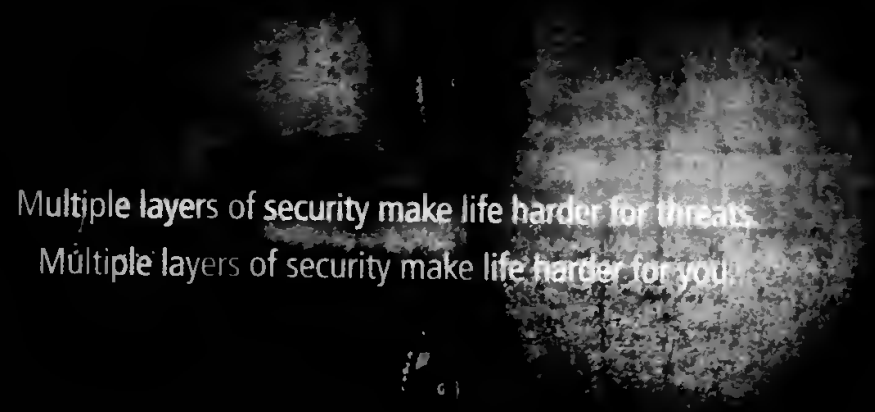
Avoid Spending Fatigue

How to stoke the security funding fires and articulate the value of resources already spent. **By Mary Brandel**

XEROX CORP. takes information security pretty seriously. It regularly conducts network vulnerability scans, as well as corporate audits of its risk mitigation efforts. A compliance program buoys employee awareness of its security processes — as well as its disaster recovery, information privacy and Sarbanes-Oxley Act policies — and an executive board champions adherence to them all. Meanwhile, the security budget at the Stamford, Conn.-based company is holding steady compared with last year, even as its other IT spending is down.

And yet, as Xerox Chief Security Officer Audrey Pantas says, "you never get as much you'd like — you could

Continued on page 36


Multiple layers of security make life harder for threats.
Multiple layers of security make life harder for you.

Continued from page 34

always do more." And that sums up the mind-set surrounding IT security at corporations today: No matter how much money you pour into it, you'll always need to go back to the well.

With growing threats, increased regulations and plenty of media coverage when incidents do occur, executives have never been more aware of the importance of IT security. At the same time, spending fatigue may be creeping into the boardroom, as CXOs increasingly look for the business value earned on the security dollars spent.

"Senior management knows there's a problem, but it seems that every day the problem gets worse, and it's like there's no end in sight," says Robert Charette, director of the enterprise risk management and governance practice at Cutter Consortium, an IT consultancy in Arlington, Mass. "There's the feeling that they could give security every single penny and it still wouldn't be enough."

To keep the security budget from looking like a black hole, you need to articulate the value of the money being spent. Here are some do's and don'ts for doing just that.

DON'T Use Scare Tactics

Every day, it seems, a story emerges about a backup-tape theft or compromised customer data. But don't overuse these incidents when seeking to justify your funding requests. "CXOs can become desensitized or jaded if they hear too much about reports that they don't think affect them," says Christopher Bomar, founder of Boomarang LLC, an online data-backup service firm in Cincinnati.

"FUD has been used up," agrees Mark Rhodes-Ousley, an information security architect and author of *Network Security: The Complete Reference* (McGraw-Hill Osborne Media, 2003). "So many people have cried wolf that executives are inured to scary stories."

You might, however, consider using recent security incidents to shed light on your company's needs. For instance, you can send out regular e-mails that put news stories into perspective and show how they apply — or don't — to your business, says Bob Dehnhardt, network and information security manager at TriNet, a human resources services firm in San Leandro, Calif. "You can use these incidents as an opening, but back them up with a strong business case," he says.

For instance, when a report comes out about backup tapes being stolen, point out what happened to the company's stock price on the day the story broke, says Gary McGraw, chief technology officer at security consultancy Cigital Inc. and author of *Software Security: Building Security In* (Addison-Wesley Professional, 2006).

DO Use Horizon Planning

Instead of asking for funding several times a year, project the security costs that need to be incurred over a 12-to-24-month time horizon, Rhodes-Ousley says. "CXOs can swallow that more easily," he says. "If you say you need certain things next year, you can get funding more easily than saying you need something now."

At Xerox, Pantas develops a three-to-four-year strategic plan for the company's security efforts and then prioritizes which of those projects to pursue in the ensuing year. "I do work off an overall strategic plan on where we want to take security," she says.

DO Let the CXO Define Acceptable Risk

Business executives deal with risk all the time, so before forking over money for protecting corporate systems and data, they first want to know the degree of legal, financial, operational and strategic risk they're facing. Only then can they decide how much they need to mitigate their exposure and, thus, how much they want to spend.

"If the CIO is bringing concrete evidence of exposure, liability and even an actual incident, the discussion changes from 'Should we do this?' to 'How much would it cost to make this go away?' " Bomar says.

When you present this information, give the executives an array of choices with different levels of protection — like they'd get when choosing an insurance plan, Charette says. "Let them understand what's at risk and then let them choose how much they want to cover themselves," he says.

Doug Lewis, a former CIO and a senior partner at The Edge Consulting Group LLC in Atlanta, calls this "finding the prudent zone." He recommends adding up how much it would cost to improve security and then plotting the range of spending options on a chart. On one side of the chart is the "danger zone," where security is insufficient, and on the other is the "ridiculous zone," where the company is overspending. Somewhere in the middle, he says, is the prudent zone, which will vary depending on your industry and security risks.

"You have to explain that if you're manufacturing talcum powder, you're probably not a big target for intellectual property theft, compared to a health care firm or a bank," Lewis says. "You have to take a balanced, prudent view and not overbill the case."

DO Use Business Language

When you live and breathe security, it's easy to be passionate about things like the difference between intrusion protection and intrusion detection. But don't bring that talk into a board meeting. "You have to explain yourself in human-readable terms," Lewis says. "What the CEO wants to know is, 'Am I being protected at a prudent level, and if not, what do I need to do to get there?' "

When Pantas discusses the importance of avoiding vulnerability in soft-

Continued on page 39

Regulatory Driver

THERE'S NOTHING LIKE a regulation to help justify security expenditures. Nothing shapes a funding argument quite so well as the threat of fines, jail or marred reputation resulting from regulatory noncompliance.

However, IT has to be careful about how hard and how often it pushes the compliance button. One reason is that organizations are increasingly appointing people specifically for that job, and IT should work with them — as well as with the legal department, auditing and internal risk management — and base security investments on the decisions that come out of those bodies.

"I've had feedback that it sometimes looks like IT or the security department is the tail trying to wag the compliance dog," says Tom Scholtz, an analyst at Gartner. "IT should be a key partner but shouldn't hijack the debate and lead the effort."

In particular, Scholtz warns, don't use compliance as an excuse for security projects that otherwise wouldn't have been justified.

In other words, "coordinate but don't duplicate," according to Robert Charette, director of the enterprise risk management and governance practice at Cutter Consortium.

At the same time, it can be frustrating to stand by and watch as your company refuses to make investments in securing areas that aren't regulated.

"I have designed security for dozens of companies, and none of them have ever secured anything they didn't absolutely have to, especially customer data," says Mark Rhodes-Ousley, an information security architect. "Even the simple precaution of encryption is almost never practiced."

With the possibility of regulations requiring encryption on hard drives looming on the horizon, Rhodes-Ousley is starting to see companies deploy encryption on their endpoint workstations. "This is only a beginning, but I'm hopeful," he says.

"It shouldn't take a federal law to make a company start caring about how the personal information that they've been trusted with is being handled," says Christopher Bomar, founder of Boomarang. "But unfortunately, that's how companies are operating now as a majority."

– MARY BRANDEL

Continued from page 34

always do more." And that sums up the mind-set surrounding IT security at corporations today: No matter how much money you pour into it, you'll always need to go back to the well.

With growing threats, increased regulations and plenty of media coverage when incidents do occur, executives have never been more aware of the importance of IT security. At the same time, spending fatigue may be creeping into the boardroom, as CXOs increasingly look for the business value earned on the security dollars spent.

"Senior management knows there's a problem, but it seems that every day the problem gets worse, and it's like there's no end in sight," says Robert Charette, director of the enterprise risk management and governance practice at Cutter Consortium, an IT consultancy in Arlington, Mass. "There's the feeling that they could give security every single penny and it still wouldn't be enough."

To keep the security budget from looking like a black hole, you need to articulate the value of the money being spent. Here are some do's and don'ts for doing just that.

DON'T Use Scare Tactics

Every day, it seems, a story emerges about a backup-tape theft or compromised customer data. But don't overuse these incidents when seeking to justify your funding requests. "CXOs can become desensitized or jaded if they hear too much about reports that they don't think affect them," says Christopher Bomar, founder of Boomarang LLC, an online data-backup service firm in Cincinnati.

"FUD has been used up," agrees Mark Rhodes-Ousley, an information security architect and author of *Network Security: The Complete Reference* (McGraw-Hill Osborne Media, 2003). "So many people have cried wolf that executives are inured to scary stories."

You might, however, consider using recent security incidents to shed light on your company's needs. For instance, you can send out regular e-mails that put news stories into perspective and show how they apply — or don't — to your business, says Bob Dehnhardt, network and information security manager at TriNet, a human resources services firm in San Leandro, Calif. "You can use these incidents as an opening, but back them up with a strong business case," he says.

For instance, when a report comes out about backup tapes being stolen, point out what happened to the company's stock price on the day the story broke, says Gary McGraw, chief technology officer at security consultancy Cigital Inc. and author of *Software Security: Building Security In* (Addison-Wesley Professional, 2006).

DO Use Horizon Planning

Instead of asking for funding several times a year, project the security costs that need to be incurred over a 12-to-24-month time horizon, Rhodes-Ousley says. "CXOs can swallow that more easily," he says. "If you say you need certain things next year, you can get funding more easily than saying you need something now."

At Xerox, Pantas develops a three-to-four-year strategic plan for the company's security efforts and then prioritizes which of those projects to pursue in the ensuing year. "I do work off an overall strategic plan on where we want to take security," she says.

DO Let the CXO Define Acceptable Risk

Business executives deal with risk all the time, so before forking over money for protecting corporate systems and data, they first want to know the degree of legal, financial, operational and strategic risk they're facing. Only then can they decide how much they need to mitigate their exposure and, thus, how much they want to spend.

"If the CIO is bringing concrete evidence of exposure, liability and even an actual incident, the discussion changes from 'Should we do this?' to 'How much would it cost to make this go away?' " Bomar says.

When you present this information, give the executives an array of choices with different levels of protection — like they'd get when choosing an insurance plan, Charette says. "Let them understand what's at risk and then let them choose how much they want to cover themselves," he says.

Doug Lewis, a former CIO and a senior partner at The Edge Consulting Group LLC in Atlanta, calls this "finding the prudent zone." He recommends adding up how much it would cost to improve security and then plotting the range of spending options on a chart. On one side of the chart is the "danger zone," where security is insufficient, and on the other is the "ridiculous zone," where the company is overspending. Somewhere in the middle, he says, is the prudent zone, which will vary depending on your industry and security risks.

"You have to explain that if you're manufacturing talcum powder, you're probably not a big target for intellectual property theft, compared to a health care firm or a bank," Lewis says. "You have to take a balanced, prudent view and not overbill the case."

DO Use Business Language

When you live and breathe security, it's easy to be passionate about things like the difference between intrusion protection and intrusion detection. But don't bring that talk into a board meeting. "You have to explain yourself in human-readable terms," Lewis says. "What the CEO wants to know is, 'Am I being protected at a prudent level, and if not, what do I need to do to get there?' "

When Pantas discusses the importance of avoiding vulnerability in soft-

Continued on page 39

Regulatory Driver

THERE'S NOTHING LIKE a regulation to help justify security expenditures. Nothing shapes a funding argument quite so well as the threat of fines, jail or marred reputation resulting from regulatory noncompliance.

However, IT has to be careful about how hard and how often it pushes the compliance button. One reason is that organizations are increasingly appointing people specifically for that job, and IT should work with them – as well as with the legal department, auditing and internal risk management – and base security investments on the decisions that come out of those bodies.

"I've had feedback that it sometimes looks like IT or the security department is the tail trying to wag the compliance dog," says Tom Scholtz, an analyst at Gartner. "IT should be a key partner but shouldn't hijack the debate and lead the effort."

In particular, Scholtz warns, don't use compliance as an excuse for security projects that otherwise wouldn't have been justified.

In other words, "coordinate but don't duplicate," according to Robert Charette, director of the enterprise risk management and governance practice at Cutter Consortium.

At the same time, it can be frustrating to stand by and watch as your company refuses to make investments in securing areas that aren't regulated.

"I have designed security for dozens of companies, and none of them have ever secured anything they didn't absolutely have to, especially customer data," says Mark Rhodes-Ousley, an information security architect. "Even the simple precaution of encryption is almost never practiced."

With the possibility of regulations requiring encryption on hard drives looming on the horizon, Rhodes-Ousley is starting to see companies deploy encryption on their endpoint workstations. "This is only a beginning, but I'm hopeful," he says.

"It shouldn't take a federal law to make a company start caring about how the personal information that they've been trusted with is being handled," says Christopher Bomar, founder of Boomarang. "But unfortunately, that's how companies are operating now as a majority."

– MARY BRANDEL

Have You Unlocked the True Value of Business Intelligence?

Computerworld's IT Management Summit Can Show You How

Why do some companies thrive and prosper by leveraging business intelligence, while others can't seem to find the value? In today's competitive marketplace, maximizing business performance can be directly related to understanding how to unlock the potential of business intelligence. And understanding this potential can be learned by simply seeing how others have succeeded.

Apply to attend Computerworld's complimentary* half-day IT Management Summit: Unlocking the Value of Business Intelligence: Keys to Maximizing Business Performance.

* Complimentary registration is restricted to qualified IT directors and managers only.

Apply for registration today
Contact Jean Lee at 888-299-0155
or visit: **www.itmanegementsummit.com**

May 10, 2006 • Chicago, Illinois

Metropolitan Club • Oak Room • Sears Tower, 66th Floor

Unlocking the Value of Business Intelligence: Keys to Maximizing Business Performance

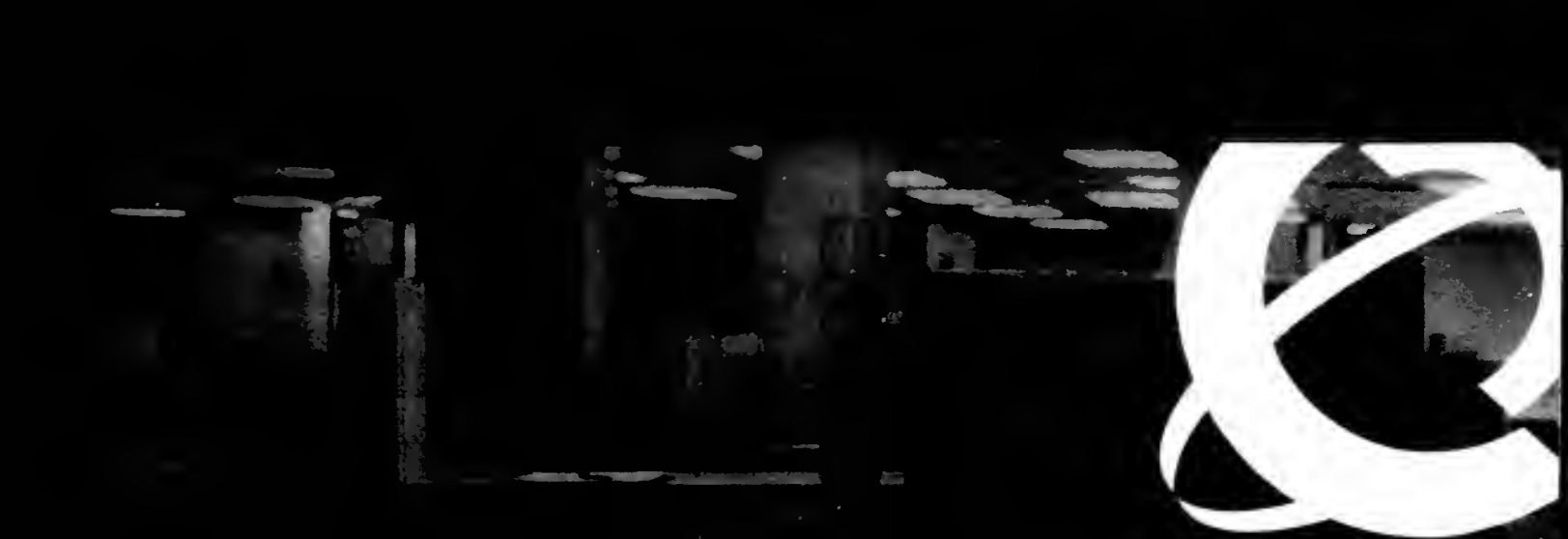
8:00am to 8:30am	**Registration and Networking Breakfast**
8:30am to 8:40am	**Introduction and Overview** Ron Milton, Executive Vice President, Computerworld
8:40am to 9:20am	**Market Overview and Trends** Bill Hostmann, featured Research Vice President, Gartner
9:20am to 10:00am	**Competing on Analytics** Thomas Davenport, President's Distinguished Professor, Babson College
10:00am to 10:15am	**Refreshment and Networking Break**
10:15am to 10:50am	**Strategies for Improving Information Management** Keith Collins, Senior Vice President and Chief Technology Officer, SAS
10:50am to 11:25am	**The Top Ten Success Factors in Business Intelligence** Gregory McMillan, Senior Manager, IT Systems, Ford Motor Company
11:25am to Noon	**BI at Pfizer: A Case Study** Danny Siegel, Senior Manager, Business Technology, Pfizer Health Solutions
Noon	**Optional Luncheon and Presentation** Bill Hostmann, featured Research Vice President, Gartner

COMPUTERWORLD
IT MANAGEMENT SUMMIT
BUSINESS INTELLIGENCE

Exclusively sponsored by

sas. The Power to Know.

intel



ROCKET SCIENCE

> MADE SIMPLE

Convergence. It's not rocket science. In fact, it's a much simpler way to do business. As a leader in convergence, we're helping businesses worldwide cut communications costs up to 60%, all while increasing productivity. How brilliant.

>BUSINESS MADE **SIMPLE**

nortel.com

NORTEL

Continued from page 36

ware code, for instance, she doesn't go off on a tangent about not doing cross-site scripting, she says.

So instead of saying things like "threat detection," "encryption" and "data protection," use terms like, "exposure," "indemnity," "protecting the brand" and "effect on market cap," says Tom Scholtz, an analyst at Gartner Inc.

For instance, if your company just launched a branding campaign for its product or service, brand protection is a relevant justification for security spending. "You say, 'You guys spent $200 million last year on branding your credit card as the cool card to carry around, and one story in *The Wall Street Journal* can bring that all tumbling down,' " McGraw says. "Then, if someone says, 'Why did we install that expensive apparatus?' you can say, 'Because we're protecting the brand.' "

And you had better be able to state your case in an "elevator speech" — a concise, compelling argument that can be made in less than a minute. "What's that one message?" Charette says. "They don't care about the different levels of encryption — they care about the harm it will keep the company from suffering and how much it's exposed in the different scenarios."

DON'T Use ROI Arguments

Investing in security rarely yields a return on investment, so promising an ROI will sound ill-informed to a senior executive. "You really have to talk about it from an insurance perspective," Pantas says. "It's more about cost avoidance or cost of compliance; there's very little in what we do that's relative to gaining ROI."

It's possible to discuss other benefits of security spending, such as protecting the company's ability to generate revenue, keep market share or retain its reputation. But ROI relates to expanding revenue and profits, "and security isn't about that," Charette says. "Trying to sell it as if it's a revenue generator is a good way to have the board say, 'Are you nuts?' "

DO Report on Benefits From Past Spending

Before asking for more security funding, make sure you close the loop on your previous spending by regularly updating executives on the results of those efforts. This means regularly measuring things like how many malicious attempts were stopped at the firewall or how quickly incidents were resolved and summarizing this data in a meaningful way.

Pantas has her team conduct regular audits on network attacks, providing her not only with an idea of where vulnerabilities continue to exist but also with a record of improvement over time.

> [Senior executives] don't care about the different levels of encryption – they care about the harm it will keep the company from suffering and how much it's exposed in the different scenarios.

"After you've invested in new security technology, you need to come back six months later and show what you've achieved and how it squares up with what you intended to achieve," Scholtz says.

You also need metrics to show that it's good when nothing happens, McGraw says. For instance, following a worm outbreak, use network-activity reporting to show that you had the proper protective measures in place. Otherwise, you can fall into the chicken-and-egg trap, where people begin wondering why you have to keep investing in security when nothing had ever happens.

McGraw also cautions against getting too granular in your reporting efforts. "They don't want to see your firewall logs or the number of virus scans or something geeky that you have to explain in three paragraphs," he says. "What they want to know is they invested $10 million in this product line and it's not going to be hacked on the first day."

Unfortunately, the most reliable way to ensure security funding is through regulation, "and that's a shame," Rhodes-Ousley laments. "Businesses simply won't do the right thing, such as protecting customer identities and private information, if they're not required to." The best thing to do in those instances, Scholtz says, is to partner with the internal compliance organization. "Complying with regulations has very direct consequences for information security and IT," he says. "But it's really the business that needs to make the risk-based decision on what they're going to do."

Brandel is a Computerworld *contributing writer. Contact her at marybrandel@verizon.net.*

Top Secret

Classification helps flag and secure sensitive data, but it can be a labor-intensive exercise.

By Jennifer McAdams

MUCKING UP the best-laid security plans everywhere is the messy issue of how enterprises are supposed to cope with staggering amounts of unstructured data, some of it for internal eyes only, such as ad hoc files generated by e-mail and other applications. It's a huge problem that only the smallest of vendors right now are ready to tackle.

Many technology executives are taking note of the new breed of data classification or information content management (ICM) offerings, which promise to help set policies and access controls on sensitive data buried in unruly, unstructured data sets. Vendors are positioning ICM storage software as an alternative to labor-intensive content management or metadata tools.

Holding back ICM adoption rates, however, is the newcomer status of data classification vendors and the level of complexity sometimes involved in harnessing ICM for security enhancement, according to several market analysts and enterprise IT officials now exploring the data classification market.

"ICM tools can help define security-sensitive data and prevent it from being incorrectly exposed," says Mayur Raichura, managing director of information services at Fairfax, Va.-based real estate company The Long & Foster Cos. "If correctly done, ICM tools can provide reasonable assurances that [sensitive] data is not exposed."

Finding a Balance

Yet in Raichura's opinion, correct use of ICM products can easily amount to extra work for enterprise IT shops. "How are you going to get expert users to identify and classify terabytes' worth of data, most of it unstructured, when they have regular jobs to do? Without a doubt, it can be done with the right allocation of resources," he says.

For Long & Foster, the tremendous amount of coding and testing work the company conducts offshore is a rapidly swelling source of unstructured data. "This data has expanded without any significant structure or classification. While it is secure at basic levels, much needs to be done," Raichura says.

Given the amount of unstructured data that Raichura and others are forced to contend with, further allocation of resources isn't an option and is precisely why senior IT officials are poking around the ICM market in the first place, according to analysts such as IDC's Laura DuBois.

"In talking to users, there are several key challenges they face that are driving interest in these products. The first is the sheer growth of data," she says. According to IDC, enterprises will see a staggering 52% growth in data over the next year — much of it an increase in unstructured data. Besides data volume spikes, security concerns — especially in the area of compliance — are spurring interest in ICM, DuBois adds.

"Large firms are evaluating more automated ways in which to classify data and, in particular, unstructured data. A manual method is just not viable, given the number of files and the distributed nature of files," she says.

Manual Labor

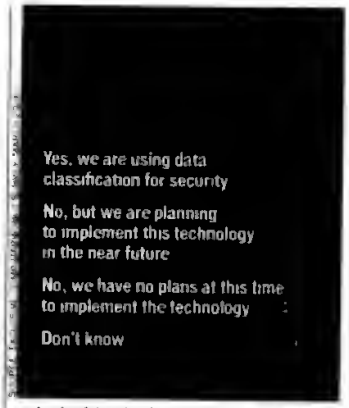
While Long & Foster toils over the security and storage of software coding data, IT officials at George Washington University (GWU) in Washington are scratching their heads over the best way to secure e-mail and other ad hoc files. "I think there is a lot more out there than we are giving credit to. And right now, we are just not able to treat this unstructured data with the rigor we do official hard copies of information," says Dave Swartz, the university's vice president and CIO.

GWU worked hard for years to assign security levels and storage procedures to its many structured data sets and has created a universitywide data-classification policy. "First, we had to get the basics in place," says Swartz. GWU relies on EMC Corp.'s Symmetrix DMX series of network-attached storage products to categorize and apply security policies to its structured data, which includes legal documents, contracts and grant-related information.

More confounding has been unstructured data, Swartz says. "We have manually designated folders and set up an encrypted archive to put e-mail and other files into a document management system. So we are able to intelligently drag and drop files into the proper folders. We understand what we are doing, but it is not automatic," he says.

Swartz says he is aware of and interested in the growing class of ICM vendors. However, GWU's adoption of their tools is still a ways off.

Indeed, most enterprises seem only to be inching in the direction of ICM. "The question for the enterprise is, What makes sense, and at what time?" says Brad O'Neill, an analyst at Taneja Group in Hopkinton, Mass.



The decision about whether or when to adopt ICM could have much to do with how difficult it is to improve the security of unclassified data through the use of these new products, O'Neill says. "Setting security policies can range from very easy to incredibly complex, depending on the number of variables and scale of informational security desired," he says.

Because of product complexity, a content management approach still makes sense to some enterprises. "Too often, there is a rush to try to apply structure to unstructured content. Anecdotal evidence suggests these efforts don't always address all business requirements," says Scott Bentivegna, project manager for knowledge management at Washington Group International Inc., a Boise, Idaho-based engineering, construction and management solutions provider. The firm uses EMC's Documentum content management system for its unstructured data.

The perceived lack of maturity among ICM vendors has much to do with sluggish adoption rates, says O'Neill. "To me, this is very much an emerging category," he says, although he is quick to add that ICM's appeal can be very powerful, especially on a security level.

Despite the newcomer status of ICM vendors, enterprises scrambling to secure unstructured data will want to watch these small players carefully. Analysts predict that many ICM product vendors will soon make significant corporate inroads.

McAdams is a freelance writer in Vienna, Va. Contact her at jjwriterva@aol.com.

Automatic Flaggers

A HANDFUL of emerging ICM companies are marching out data classification tools that can purportedly automatically crack open any unstructured file, seize its sensitive content, impose critical security policies and dispatch the data to appropriate storage tiers.

Two of these newcomers have nailed partnerships with large storage vendors. Network Appliance Inc. has teamed with Kazeon Systems Inc., which offers Kazeon IS1200, a product designed to eliminate manual classification tasks. Meanwhile, Arkivio Inc. has formed an alliance with EMC.

According to analysts, other ICM companies to watch include Abrevity Inc., Trusted Edge Inc., Njini Inc., StoredIQ Corp. and Index Engines Inc.

– JENNIFER McADAMS

Top Secret

Classification helps flag and secure sensitive data, but it can be a labor-intensive exercise.

By Jennifer McAdams

MUCKING UP the best-laid security plans everywhere is the messy issue of how enterprises are supposed to cope with staggering amounts of unstructured data, some of it for internal eyes only, such as ad hoc files generated by e-mail and other applications. It's a huge problem that only the smallest of vendors right now are ready to tackle.

Many technology executives are taking note of the new breed of data classification or information content management (ICM) offerings, which promise to help set policies and access controls on sensitive data buried in unruly, unstructured data sets. Vendors are positioning ICM storage software as an alternative to labor-intensive content management or metadata tools.

Holding back ICM adoption rates, however, is the newcomer status of data classification vendors and the level of complexity sometimes involved in harnessing ICM for security enhancement, according to several market analysts and enterprise IT officials now exploring the data classification market.

"ICM tools can help define security-sensitive data and prevent it from being incorrectly exposed," says Mayur Raichura, managing director of information services at Fairfax, Va.-based real estate company The Long & Foster Cos. "If correctly done, ICM tools can provide reasonable assurances that [sensitive] data is not exposed."

Finding a Balance

Yet in Raichura's opinion, correct use of ICM products can easily amount to extra work for enterprise IT shops. "How are you going to get expert users to identify and classify terabytes' worth of data, most of it unstructured, when they have regular jobs to do? Without a doubt, it can be done with the right allocation of resources," he says.

For Long & Foster, the tremendous amount of coding and testing work the company conducts offshore is a rapidly swelling source of unstructured data. "This data has expanded without any significant structure or classification. While it is secure at basic levels, much needs to be done," Raichura says.

RICK ILLARD

Given the amount of unstructured data that Raichura and others are forced to contend with, further allocation of resources isn't an option and is precisely why senior IT officials are poking around the ICM market in the first place, according to analysts such as IDC's Laura DuBois.

"In talking to users, there are several key challenges they face that are driving interest in these products. The first is the sheer growth of data," she says. According to IDC, enterprises will see a staggering 52% growth in data over the next year — much of it an increase in unstructured data. Besides data volume spikes, security concerns — especially in the area of compliance — are spurring interest in ICM, DuBois adds.

"Large firms are evaluating more automated ways in which to classify data and, in particular, unstructured data. A manual method is just not viable, given the number of files and the distributed nature of files," she says.

Manual Labor

While Long & Foster toils over the security and storage of software coding data, IT officials at George Washington University (GWU) in Washington are scratching their heads over the best way to secure e-mail and other ad hoc files. "I think there is a lot more out there than we are giving credit to. And right now, we are just not able to treat this unstructured data with the rigor we do official hard copies of information," says Dave Swartz, the university's vice president and CIO.

GWU worked hard for years to assign security levels and storage procedures to its many structured data sets and has created a universitywide data-classification policy. "First, we had to get the basics in place," says Swartz. GWU relies on EMC Corp.'s Symmetrix DMX series of network-attached storage products to categorize and apply security policies to its structured data, which includes legal documents, contracts and grant-related information.

More confounding has been unstructured data, Swartz says. "We have manually designated folders and set up an encrypted archive to put e-mail and other files into a document management system. So we are able to intelligently drag and drop files into the proper folders. We understand what we are doing, but it is not automatic," he says.

Swartz says he is aware of and interested in the growing class of ICM vendors. However, GWU's adoption of their tools is still a ways off.

Indeed, most enterprises seem only to be inching in the direction of ICM. "The question for the enterprise is, What makes sense, and at what time?" says Brad O'Neill, an analyst at Taneja Group in Hopkinton, Mass.

The decision about whether or when to adopt ICM could have much to do with how difficult it is to improve the security of unclassified data through the use of these new products, O'Neill says. "Setting security policies can range from very easy to incredibly complex, depending on the number of variables and scale of informational security desired," he says.

Because of product complexity, a content management approach still makes sense to some enterprises. "Too often, there is a rush to try to apply structure to unstructured content. Anecdotal evidence suggests these efforts don't always address all business requirements," says Scott Bentivegna, project manager for knowledge management at Washington Group International Inc., a Boise, Idaho-based engineering, construction and management solutions provider. The firm uses EMC's Documentum content management system for its unstructured data.

The perceived lack of maturity among ICM vendors has much to do with sluggish adoption rates, says O'Neill. "To me, this is very much an emerging category," he says, although he is quick to add that ICM's appeal can be very powerful, especially on a security level.

Despite the newcomer status of ICM vendors, enterprises scrambling to secure unstructured data will want to watch these small players carefully. Analysts predict that many ICM product vendors will soon make significant corporate inroads.

Automatic Flaggers

A HANDFUL of emerging ICM companies are marching out data classification tools that can purportedly automatically crack open any unstructured file, seize its sensitive content, impose critical security policies and dispatch the data to appropriate storage tiers.

Two of these newcomers have nailed partnerships with large storage vendors. Network Appliance Inc. has teamed with Kazeon Systems Inc., which offers Kazeon IS1200, a product designed to eliminate manual classification tasks. Meanwhile, Arkivio Inc. has formed an alliance with EMC.

According to analysts, other ICM companies to watch include Abrevity Inc., Trusted Edge Inc., Njini Inc., StoredIQ Corp. and Index Engines Inc.

– JENNIFER McADAMS

McAdams is a freelance writer in Vienna, Va. Contact her at jjwriterva@aol.com.

Beyond Posters

Your employees need more than slogans. Here are some other ways to get them to take security seriously. By Mary K. Pratt

IT'S THE kind of breach that companies fear: workers giving out network log-in names or changing passwords when asked to by someone posing as an IT staffer. The best firewalls on the market can't protect against such scenarios.

"Why even lock your doors if employees happily hold them open for a stranger following behind them?" asks Alex Ryan, security officer at VeriCenter Inc., an IT infrastructure and managed services provider in Houston.

The risk that employees pose is significant. They can fall prey to social engineering, a fancy term for being conned. They can ignore company policy by failing to encrypt sensitive data. Or they might install unauthorized software that can corrupt the system.

Think you're well protected? Recent findings from the Computing Technology Industry Association might convince you otherwise. In this year's CompTIA information security study, 59% of the organizations surveyed indicated that their latest security breaches were the result of human error alone. That's up from 47% last year.

Despite such statistics, many companies fail to do enough to educate their workers. That's what the Internal Revenue Service discovered, according to a March 2005 federal government report.

Federal inspectors posing as IT help desk staffers trying to correct a network problem called 100 IRS managers and employees and asked them to provide their network log-in names and temporarily change their passwords to ones they suggested. Inspectors persuaded 35 IRS workers to do just that.

This success came despite IRS efforts to educate employees.

Dan Galik, the IRS's chief security officer, says his agency "re-energized the awareness program" following the report. In addition to annual reviews, posted announcements and online courses mandated under the 2002 Federal Information Security Management Act, Galik says the agency has added some innovative approaches. One was a *Jeopardy*-style game held last November during which workers tried to give the right answers on security-related topics. "You've got to come up with something that will stick," Galik says.

Here are some other practices that have proved effective in getting the message across.

Make It Personal

"Many employees worry about their home machines' security. Leverage that concern to promote general security

Continued on page 44

Continued from page 42

principles that can be applied at both home and work," Ryan says. "It's a way to make people personally interested in security." She e-mails employees newsletters with tips that alert them to the latest scams or viruses that could affect both their work and personal PCs.

Companies can also use personal examples to show what they're trying to achieve on a corporate level, says IT security expert Candy Alexander, a consultant at Alexander Advisory LLC in Merrimack, N.H. For example, companies can tell workers that protecting passwords is no less important than protecting their debit cards' PINs.

If you have the luxury of getting people into a classroom for training, Ryan recommends a little live action to drive home the message. She has enlisted students during classes to act out roles, such as a hacker and an administrative assistant. She instructs the hacker to pressure the assistant for his computer password with techniques that real-life social engineers use.

Companies also shouldn't underestimate the power of publicity, says IT security expert Jim Litchko. He points to a situation that played out at a government intelligence agency where a senior official, against agency policy, brought in a disk that turned out to contain a virus. The agency fired him and let everyone know it.

"To those people who value their jobs, it's very effective" in highlighting the importance of security, says Litchko, president of Litchko & Associates Inc., an IT consulting firm in Kensington, Md., and past chairman of the IT security council for ASIS International, an organization of security professionals.

Employees should also have simple steps to follow if they suspect security problems. Litchko says one company had stickers on its computers providing information on typical scams, along with a number to call for help.

Integrate Security Awareness

Companies that consider security training an annual event are missing out on opportunities to make security part of the everyday culture, says Jonathan G. Gossels, president of SystemExperts Corp., a Sudbury, Mass.-based network security consulting firm.

Gossels recommends leveraging ongoing training events. He notes that one client, a large chemical company, incorporates security components into its regular professional development courses. "No one would take time out to take a security course, but to take 15 minutes in another course works well. And they're able to tune the security message to the people taking the course," Gossels says.

Also, don't let security become an "out of sight, out of mind" issue, says Litchko. "It has to be a continual thing. You can't just put up a poster and keep it there a year. It needs to be constant and varied."

In addition to her monthly security newsletters, VeriCenter's Ryan regularly e-mails summaries of news articles related to IT security.

Another way to keep security on everyone's mind is to use technology itself to remind them, says Joel Rakow, the e-crimes practice leader at Tatum LLC, an executive consulting and services firm in Atlanta. Companies can have security-related tips and reminders — like "Our data is sensitive information," or "Customer information is available on a need-to-know basis" — flash up on screensavers.

Like so much else in IT, security training should not take a one-size-fits-all approach, says Susan Hansche, program manager at Nortel Government Solutions Inc., a Fairfax, Va.-based company that provides information-assurance training programs to the U.S. Department of State.

Hansche recommends role-based training, where the messages and action items are targeted to specific audiences. Her company, for example, uses eight different role-based programs to train 1,000 State Department employees annually. The courses for executives are different from those for senior-level managers and general end users.

Alexander has taken a similar approach to training. She says executives like war stories, middle managers prefer presentations that give them checklists of action items, and general end users like information in small, easily digestible chucks.

When Alexander worked at the former Digital Equipment Corp., she developed a scavenger hunt that asked workers to find 10 items related to security on the company's Web site.

Those who got all 10 were entered into a drawing to win a mug.

You might be surprised to learn that the nonmandatory event drew in more than 70% of the company's worldwide workforce. "Positive competition is really beneficial," Alexander says.

K Rudolph says she has seen similar success with competitive programs. Rudolph is a Certified Information Systems Security Professional and chief inspiration officer at Native Intelligence Inc., a company in Glenelg, Md., that provides IT security awareness services to government agencies and private industry.

She says one of her clients implemented a "news hawk" program, where the first employee to bring in a news story on IT security gets a prize. Prizes have ranged from time off to movie tickets. The awareness team then distributes the news item through a weekly e-mail or its periodic newsletter.

Make It Fun

IT security is a serious topic, but security officials have found that some levity helps keep workers' attention.

Alexander, like many others, has used Web-based training to educate employees on security topics and used online quizzes to test their knowledge. Although the material covered significant topics, she still found ways to elicit some smirks. For example, the multiple-choice answers for "What is social engineering?" included "a college degree" and "a job on a cruise line" — obviously false answers infused with a hint of dry wit.

"It's not extremely silly," Alexander says, "but it's something to make people remember."

Pratt is a Computerworld contributing writer in Waltham, Mass. Contact her at marykpratt@verizon.net.

Would Your Workers Pass the Test?

As an executive at an IT consulting company, Bruce Baird assumed that his workers were security-savvy. But a conversation with a former colleague rocked his confidence.

Baird, vice president of operations at T2 Software Services Inc. in Tampa, Fla., learned from security expert Todd Snapp that hackers can set up phones to spoof the Caller ID names of legitimate companies.

"One of the things we look for when we hire consultants is interpersonal skills – [people who ask] 'How can I help you?' when talking to clients. And if they think they're talking to the client and they're really not," they could be unintentionally passing along information to hackers, Baird says.

Companies have used so-called penetration testing to see how well their technology can fend off intruders. Some are now using the same techniques to see how well their employees can spot potential problems. The results, according to reports, aren't encouraging.

"We have found that a lot of companies spend a lot of money and time building a strong, secure infrastructure, but they don't spend much time on securing their people. They're not trained on what to look for, at a time when hackers are getting more sophisticated," says Snapp, president of RocketReady, a Tampa company that offers readiness testing in addition to other services and products.

RocketReady's employees use the same techniques that malicious hackers use to gain information and access to a company's IT infrastructure and the data it contains.

They gather information from readily available sources, such as a company's Web site. They then pose as customers, potential clients, representatives of partner companies, travel agents and even employees to get specific details, such as employee ID numbers and acronyms used only by company workers, that will help them in their attacks.

Baird doesn't want T2 employees to fall prey to scams. Since RocketReady showed him how easily it could spoof Caller ID, Baird has upped company-sponsored training on this issue and now requires staffers to take annual courses on the topic.

– MARY K. PRATT

Continued from page 42

principles that can be applied at both home and work," Ryan says. "It's a way to make people personally interested in security." She e-mails employees newsletters with tips that alert them to the latest scams or viruses that could affect both their work and personal PCs.

Companies can also use personal examples to show what they're trying to achieve on a corporate level, says IT security expert Candy Alexander, a consultant at Alexander Advisory LLC in Merrimack, N.H. For example, companies can tell workers that protecting passwords is no less important than protecting their debit cards' PINs.

If you have the luxury of getting people into a classroom for training, Ryan recommends a little live action to drive home the message. She has enlisted students during classes to act out roles, such as a hacker and an administrative assistant. She instructs the hacker to pressure the assistant for his computer password with techniques that real-life social engineers use.

Companies also shouldn't underestimate the power of publicity, says IT security expert Jim Litchko. He points to a situation that played out at a government intelligence agency where a senior official, against agency policy, brought in a disk that turned out to contain a virus. The agency fired him and let everyone know it.

"To those people who value their jobs, it's very effective" in highligbting the importance of security, says Litchko, president of Litchko & Associates Inc., an IT consulting firm in Kensington, Md., and past chairman of the IT security council for ASIS International, an organization of security professionals.

Employees should also have simple steps to follow if they suspect security problems. Litchko says one company had stickers on its computers providing information on typical scams, along with a number to call for help.

Integrate Security Awareness

Companies that consider security training an annual event are missing out on opportunities to make security part of the everyday culture, says Jonathan G. Gossels, president of System-Experts Corp., a Sudbury, Mass.-based network security consulting firm.

Gossels recommends leveraging ongoing training events. He notes that one client, a large chemical company, incorporates security components into its regular professional development courses. "No one would take time out to take a security course, but to take 15 minutes in another course works well. And they're able to tune the security message to the people taking the course," Gossels says.

Also, don't let security become an "out of sight, out of mind" issue, says Litchko. "It has to be a continual thing. You can't just put up a poster and keep it there a year. It needs to be constant and varied."

In addition to her monthly security newsletters, VeriCenter's Ryan regularly e-mails summaries of news articles related to IT security.

Another way to keep security on everyone's mind is to use technology itself to remind them, says Joel Rakow, the e-crimes practice leader at Tatum LLC, an executive consulting and services firm in Atlanta. Companies can have security-related tips and reminders — like "Our data is sensitive information," or "Customer information is available on a need-to-know basis" — flash up on screensavers.

Like so much else in IT, security training should not take a one-size-fits-all approach, says Susan Hansche, program manager at Nortel Government Solutions Inc., a Fairfax, Va.-based company that provides information-assurance training programs to the U.S. Department of State.

Hansche recommends role-based training, where the messages and action items are targeted to specific audiences. Her company, for example, uses eight different role-based programs to train 1,000 State Department employees annually. The courses for executives are different from those for senior-level managers and general end users.

Alexander has taken a similar approach to training. She says executives like war stories, middle managers prefer presentations that give them checklists of action items, and general end users like information in small, easily digestible chucks.

When Alexander worked at the former Digital Equipment Corp., she developed a scavenger hunt that asked workers to find 10 items related to security on the company's Web site.

Those who got all 10 were entered into a drawing to win a mug.

You might be surprised to learn that the nonmandatory event drew in more than 70% of the company's worldwide workforce. "Positive competition is really beneficial," Alexander says.

K Rudolph says she has seen similar success with competitive programs. Rudolph is a Certified Information Systems Security Professional and chief inspiration officer at Native Intelligence Inc., a company in Glenelg, Md., that provides IT security awareness services to government agencies and private industry.

She says one of her clients implemented a "news hawk" program, where the first employee to bring in a news story on IT security gets a prize. Prizes have ranged from time off to movie tickets. The awareness team then distributes the news item through a weekly e-mail or its periodic newsletter.

Make It Fun

IT security is a serious topic, but security officials have found that some levity helps keep workers' attention.

Alexander, like many others, has used Web-based training to educate employees on security topics and used online quizzes to test their knowledge. Although the material covered significant topics, she still found ways to elicit some smirks. For example, the multiple-choice answers for "What is social engineering?" included "a college degree" and "a job on a cruise line" — obviously false answers infused with a hint of dry wit.

"It's not extremely silly," Alexander says, "but it's something to make people remember."

Pratt is a Computerworld contributing writer in Waltham, Mass. Contact her at marykpratt@verizon.net.

Would Your Workers Pass the Test?

As an executive at an IT consulting company, Bruce Baird assumed that his workers were security-savvy. But a conversation with a former colleague rocked his confidence.

Baird, vice president of operations at T2 Software Services Inc. in Tampa, Fla., learned from security expert Todd Snapp that hackers can set up phones to spoof the Caller ID names of legitimate companies.

"One of the things we look for when we hire consultants is interpersonal skills – [people who ask] 'How can I help you?' when talking to clients. And if they think they're talking to the client and they're really not," they could be unintentionally passing along information to hackers, Baird says.

Companies have used so-called penetration testing to see how well their technology can fend off intruders. Some are now using the same techniques to see how well their employees can spot potential problems. The results, according to reports, aren't encouraging.

"We have found that a lot of companies spend a lot of money and time building a strong, secure infrastructure, but they don't spend much time on securing their people. They're not trained on what to look for, at a time when hackers are getting more sophisticated," says Snapp, president of RocketReady, a Tampa company that offers readiness testing in addition to other services and products.

RocketReady's employees use the same techniques that malicious hackers use to gain information and access to a company's IT infrastructure and the data it contains.

They gather information from readily available sources, such as a company's Web site. They then pose as customers, potential clients, representatives of partner companies, travel agents and even employees to get specific details, such as employee ID numbers and acronyms used only by company workers, that will help them in their attacks.

Baird doesn't want T2 employees to fall prey to scams. Since RocketReady showed him how easily it could spoof Caller ID, Baird has upped company-sponsored training on this issue and now requires staffers to take annual courses on the topic.

– MARY K. PRATT

IT ALERT:

Businesses pay most for operating and maintenance in the data center.†

Ready to simplify and save?

Insight

IT For The Way You Work™

YOU CAN MAKE IT HAPPEN WITH INSIGHT

HP ProLiant DL360 G4p
470063-702
- Intel® Xeon® Processor (2MB cache, 3GHz, 800MHz)
- Intel® Hyper-Threading Technology
- Intel® Extended Memory 64 Technology
- 2GB RAM
- 10/10/1000 Ethernet
- 3-year warranty

$1,599.00 After $500 Instant Savings

HP ProLiant DL380 G4
470063-705
- Intel® Xeon® Processor (2MB cache, 3GHz, 800MHz)
- Intel® Extended Memory 64 Technology
- 2GB RAM, CD-R
- 10/100/1000 Ethernet
- 3-year warranty

$2,149.00 After $500 Instant Savings

LIMITED TIME OFFER!
$500 INSTANT SAVINGS!

FREE INTEGRATION WITH FREE 36 GB SCSI HOT SWAP DRIVE!*
Offer Ends 05.17.06!
*Limit 5 free hard drives per customer.

insight.com/hpproliant1 • 800.767.3475

†"Changing the IT Paradigm" Intel WP

Source Code: A0047

hp invent

intel Xeon inside

Sorting The Standards

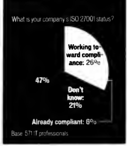
Like pieces of a puzzle, frameworks help companies meet specific security goals. By Bob Violino

M[illegible] models [illegible] than [illegible] standards.

[illegible] simply IT [illegible] functions [illegible] provide [illegible] says Kimberly Sawyer, [illegible] of computing and [illegible] at Lockheed Martin [illegible] known as Enterprise Information Systems in Orlando.

But none of the standards alone provides [illegible], Sawyer says. "They [illegible] information security concepts that must be interpreted into actions and incorporated into the daily [illegible] comprehensive security requires discipline and [illegible] across all aspects of planning, [illegible] delivery, risk management, [illegible] policy development [illegible]."

Lockheed Martin is using Cobit, ITIL and ISO 27001 for different purposes: Cobit for measuring and assessing IT controls, ITIL to improve internal IT services and ISO 27001 for IT governance. Although each helps to bolster security, none is a stand-alone solution, Sawyer says. "IT organizations must integrate the frameworks to ensure [that] best practices are integrated across the information security discipline," she says.



Here's a look at some of the key standards and their roles in a security plan.

Cobit

Developed in 1996 by the Information Systems Audit and Control Association and the IT Governance Institute, Cobit provides a framework for users and IT, security and auditing managers. It's gaining acceptance as a good practice for controlling data, systems and related risks.

"Cobit has enabled us to more sys[illegible] approach [illegible] efficiencies," says Sawyer.

The framework includes tools to measure a company's capabilities in 34 IT processes. Among them are a list of critical success factors that provides best practices for each IT process, maturity models to help in benchmarking and performance measurement elements. The standard is becoming vital as companies strive to comply with regulations such as the Sarbanes-Oxley Act.

"Cobit only has one security module, but when you look at [the standard] from a broad perspective, it addresses a lot of elements of security," says Mike Nelson, president of SecureNet Technologies Inc., a consulting firm in San Ramon, Calif., that focuses on information security. "Where it begins to break down is in providing details of the 'how.'" It gives detail of controls and objectives of controls" but doesn't explain how to implement them, he says.

ISO 27001

ISO 27001 (Information Security Management — Specification With Guidance for Use) provides more of the detail that's needed, Nelson says. The standard, which is based on an earlier standard, ISO 17799, is designed to help organizations establish and maintain effective information security controls through continual improvements.

Developed in October 2005 by the International Standards Organization, ISO 27001 implements principles of the Organization for Economic Cooperation and Development on governing the security of information and networks. The standard creates a road map for the secure design, implementation, management and maintenance of IT processes in an organization.

"ISO 27001 is a laundry list of controls; it gives more of framework for an effective security program," says Paul Proctor, an analyst at Gartner Inc. in Stamford, Conn. "Cobit and ISO 27001 are the most popular [standards] out there."

ITIL

ITIL is a set of best practices, published as books designed to help reduce the cost of using technology and to im-

Future Of NIST

ALTHOUGH [illegible] well known [illegible] the standards and [illegible] framework being [used] within the federal government could help organizations improve their security, according to information security experts.

NIST 800-53 was created in 2005 by the National Institute of Standards and Technology as required by the Federal Information Security Management Act of 2002. It provides guidelines for selecting and specifying security controls for information systems that support the executive agencies of the U.S. government.

"I believe it has the potential to do for information security what ITIL has done for service management," according to Mike Nelson, president of SecureNet Technologies.

"The NIST framework is clearly shaping up to be the state of the art for information security governance and the manifestation of due diligence," he says.

Nelson says the NIST standard provides more comprehensive security guidelines than other standards designed to enhance corporate controls and IT service levels. It's more granular than the other standards in areas such as security certification and accreditation processes, he says.

Although NIST 800-53 applies only to federal civilian agencies today, Nelson says it's designed to be generic enough to apply to the private sector.

As the standard is adopted, he predicts, "we will start to see the federal sector lead the way in terms of security governance."

BOB VIOLINO

Sorting The Standards

Like pieces of a puzzle, frameworks help companies meet specific security goals. **By Bob Violino**

MANY COMPANIES are using standards and frameworks to deal with certain aspects of information security. These models can help protect systems and data, but each plays a very different role in an overall security plan.

Some of the most popular ones, including the Control Objectives for Information and Related Technology (Cobit), ISO 27001, the IT Infrastructure Library (ITIL) and Statement on Auditing Standards (SAS) No. 70, offer guidelines for improving some elements of security. But experts say these models are more like pieces of a puzzle than comprehensive security standards.

"All of these frameworks supply IT with repeatable processes that are consistent across the various IT functions" and help technology executives provide better service, says Kimberly Sawyer, vice president of computing and network services at Lockheed Martin Corp.'s IT department, known as Enterprise Information Systems, in Orlando.

But none of the standards alone provides full security, Sawyer says. "They contain various information security concepts that must be interpreted, integrated and incorporated into the daily operations," she says. "Comprehensive security requires discipline and integration across all aspects of planning, service delivery, risk management architecture, tool selection, policy development and audits."

Lockheed Martin is using Cobit, ITIL and ISO 27001 for different purposes: Cobit for measuring and assessing IT controls, ITIL to improve internal IT services, and ISO 27001 for IT governance. Although each helps to bolster security, none is a stand-alone solution, Sawyer says. "IT organizations must integrate the frameworks to ensure [that] best practices are integrated across the information security discipline," she says.

SOURCE: ENTERPRISE MANAGEMENT ASSOCIATES, INC. • CHART: JOHN

Here's a look at some of the key standards and their roles in a security plan.

Cobit

Developed in 1996 by the Information Systems Audit and Control Association and the IT Governance Institute, Cobit provides a framework for users and IT, security and auditing managers. It's gaining acceptance as a good practice for controlling data, systems and related risks.

"Cobit has enabled us to more systematically approach audit issues to identify root causes of deficiencies," says Sawyer.

The framework includes tools to measure a company's capabilities in 34 IT processes. Among them are a list of critical success factors that provides best practices for each IT process, maturity models to help in benchmarking and performance-measurement elements. The standard is becoming vital as companies strive to comply with regulations such as the Sarbanes-Oxley Act.

"Cobit only has one security module, but when you look at [the standard] from a broad perspective, it addresses a lot of elements of security," says Mike Nelson, president of SecureNet Technologies Inc., a consulting firm in San Ramon, Calif., that focuses on information security. "Where it begins to break down is in providing details of the 'how.' It gives detail of controls and objectives of controls" but doesn't explain how to implement them, he says.

ISO 27001

ISO 27001 (Information Security Management — Specification With Guidance for Use) provides more of the detail that's needed, Nelson says. The standard, which is based on an earlier standard, ISO 17799, is designed to help organizations establish and maintain effective information security controls through continual improvements.

Developed in October 2005 by the International Standards Organization, ISO 27001 implements principles of the Organization for Economic Cooperation and Development on governing the security of information and networks. The standard creates a road map for the secure design, implementation, management and maintenance of IT processes in an organization.

"ISO 27001 is a laundry list of controls; it gives more of framework for an effective security program," says Paul Proctor, an analyst at Gartner Inc. in Stamford, Conn. "Cobit and ISO 27001 are the most popular [standards] out there."

ITIL

ITIL is a set of best practices, published as books designed to help reduce the cost of using technology and to im-

Future Of NIST

ALTHOUGH it's less well known than some of the standards and models in place at many businesses today, an emerging framework being used within the federal government could help organizations improve their security, according to information security experts.

NIST 800-53 was created in 2005 by the National Institute of Standards and Technology, as required by the Federal Information Security Management Act of 2002. It provides guidelines for selecting and specifying security controls for information systems that support the executive agencies of the U.S. government.

"I believe it has the potential to do for information security what ITIL has done for service management," according to Mike Nelson, president of SecureNet Technologies.

The NIST framework "is clearly shaping up to be the state of the art for information security governance and the manifestation of due diligence," he says.

Nelson says the NIST-standard provides more comprehensive security guidelines than other standards designed to enhance corporate controls and IT service levels. It's more granular than the other standards in areas such as security certification and accreditation processes, he says.

Although NIST 800-53 applies only to federal civilian agencies today, Nelson says it's designed to be generic enough to apply to the private sector.

As the standard is adopted, he predicts, "we will start to see the federal sector lead the way in terms of security governance."

– BOB VIOLINO

prove the quality of services delivered throughout the organization. ITIL consists of rules on how to deliver services more efficiently by improving management processes across IT departments that support networks, applications and databases.

In the late 1980s, the U.K. Office of Government Commerce developed the standards for service providers to follow in delivering IT services to the British government. ITIL covers seven main areas: service support, service delivery, planning to implement service management, infrastructure management for IT and communications technology, applications management, security management, and the business perspective.

"ITIL is strong in process management and delivery but fairly narrowly focused on those areas," says Nelson. "It only peripherally deals with security as a component in service management. From a pure security point of view, it's relatively weak, but it was not designed to address that."

Adds Proctor, "Cobit is better for meeting regulatory [requirements]. ITIL is more of an operations standard, something you use to improve the maturity of your IT operations. We find a lot of companies either choose ITIL or Cobit. Some do both, but that is rare."

Ruben Melendez says ITIL is becoming the standard of choice for many vendors and is useful for improving security. He is president of The Glomark Group Inc., a consulting firm in Columbus, Ohio, that works with IT vendors and end-user organizations to develop return-on-investment strategies.

"The companies I've worked with are all ITIL implementers," Melendez says. "We've done a lot of work with [CA] on security-related products. If you look at their literature, when they talk about security, they emphasize ITIL and not the others."

According to Melendez, other vendors pushing ITIL include Microsoft Corp., Intel Corp. and Oracle Corp.

SAS 70

SAS 70 is an auditing standard that was created by the American Institute of Certified Public Accountants (AICPA) in 1992. A SAS 70 audit shows whether an independent accounting and auditing firm has examined a service provider's controls for IT and related processes.

SAS 70 isn't a predetermined set of control objectives or activities. Auditors must follow the AICPA's standards for fieldwork, quality control and reporting and issue a formal report to the service provider that includes the auditor's opinion once the audit is completed.

There are two types of reports: one describes a service provider's controls at a specific point in time, and the other describes the controls and includes detailed testing of the service provider's control activities and processes over a minimum six-month period.

Service providers must demonstrate that they have adequate safeguards when they host or process client information. SAS 70 enables service organizations to disclose their controls to their clients and their clients' auditors in a uniform reporting format.

The benefit to companies is that they receive detailed information about a service provider's controls and an independent assessment of whether the controls are operating effectively. They can present this information to their own auditors when necessary.

SAS 70 lets organizations know if their existing controls are working, but it doesn't tell them if all the right controls are in place, Nelson says.

Each of these standards has a potential role to play in helping organizations protect their systems and data. Companies that are looking to create an overall security strategy need to explore the frameworks to see which provides the best fit.

Violino is a freelance writer in Massapequa Park, N.Y. Contact him at bviolino@optonline.net.

"Without an enterprise view, things can be missed because you can't connect the risks," says JOANNE BERKOWITZ, chief enterprise risk officer at PMI Group.

Risk Reducer

The chief risk officer takes a bird's eye view of all enterprise risk.
By John S. Webster

R[illegible] these days. [illegible] services organizations have always grappled with credit and market [illegible] risk as an integral part of doing business. But to[illegible] operation [illegible] from potential [illegible] an internal com[illegible] corporate governance [illegible] that could compromise [illegible] vertical industries and [illegible] functions, including IT. [illegible]

CAREERS

to Forrester Research Inc. in Cambridge, Mass., the executive ranks of any company that has revenue of at least $1 billion and can be classified as "critical infrastructure" — such as financial institutions, energy companies and health care providers — are likely to include a CRO. By next year, three quarters of large, critical infrastructure organizations will have a formal ERM office with a CRO or equivalent role, according to Forrester.

After its early emphasis in financial services, ERM has played an increasingly critical part in business planning across industries during the past several years. Its widespread acceptance was [illegible] in part by regulations such as the Sarbanes-Oxley Act for accounting oversight and Basel II for measurement of international banking capital. As [illegible] of operational risk also [illegible] under the ERM umbrella, [illegible] CRO's job is to eliminate the [illegible]mented approach to managing risk, according to Forrester.

With government regulations and the rise of corporate governance policies addressing enterprisewide risk, Forrester and other analyst firms have hammered on the importance of having a single point person in place to oversee its management.

"With the fragmented, siloed approach to risk management, there is no one watching risk across the organization," Forrester analyst Michael Rasmussen wrote in a December 2004 report on ERM trends. "In today's complex business world, one weak spot can impact the entire business. Without a framework to work within, and someone in charge of risk management, organizations are running in the dark."

An Expanding Role

One key to success for CROs is the ability to see the range of risk variations that can crop up across the enterprise. At The PMI Group Inc., a mortgage insurance company in Walnut Creek, Calif., the CRO position was created in 2003 to monitor international credit risk operations. But the position's description has since been expanded to encompass risk throughout the company, including strategic, operational, external, financial, IT and security (both data and physical) operations.

"Without an enterprise view, things can be missed because you can't connect the risks," says Joanne Berkowitz, chief enterprise risk officer at PMI Group. "If you're just looking at your own little world and don't have an idea of how what you're doing will affect what someone else is doing, you could [inadvertently] create risk for the company."

In IT, Berkowitz says, disaster recovery illustrates this concept.

"We have very detailed business-resumption plans and capabilities. To create these, people in the business units worked closely with me and with our CIO to identify which systems they depend on and to prioritize their recovery times," she says. "This is particularly important because an increasing proportion of our business is automated; 90% of our business now comes through systems."

James Lam, president of James Lam & Associates Inc., an enterprise risk consulting firm in Wellesley, Mass., agrees that the ability to see the big picture is key for the CRO.

"The key to success is having a strong background in the most critical risks to the company. You also have to look beyond your specific silos across the enterprise and have a comprehensive point of view," he says. "Organizations are realizing that a risk manager can help achieve a company's business objectives while he or she defends it from threats."

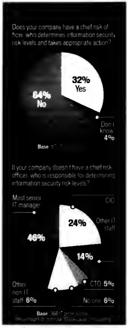
An effective CRO has a range of skills that vary depending on the business focus, says Berkowitz. "There isn't just one set of skills that will work for a CRO, and they'll vary at each company," she says.

The position requires the ability to take a holistic view of the risks that might affect operations anywhere in the company. To that end, the CRO must work with other C-level executives, as well as with business unit managers, says Berkowitz.

"We're attempting to be proactive and to adopt good governance. Here, everyone would agree that the CRO is the person who's leading that effort," she adds.

With a CRO who takes a comprehensive view of risk across an organization, ERM can become a key piece of an overall business plan. ■

Webster is a freelance writer in Providence, R.I. Contact him at john.s.webster@verizon.net.



With [illegible] things can be missed because you can't connect the risks
chief enterprise risk officer at PMI Group

Risk Reducer

The chief risk officer takes a bird's-eye view of all enterprise risk.

By John S. Webster

CAREERS

RISK IS a fact of life these days. Financial services organizations have always grappled with credit- and market-related risk as an integral part of doing business. But today, the far-reaching threat of operational risks arising from potential breakdowns in internal controls and corporate governance — breakdowns that could compromise business — span vertical industries and business functions, including IT.

With risk playing a role in many IT-related endeavors, such as data and physical security efforts and privacy and regulatory compliance initiatives, who keeps track?

Enter the chief risk officer, who acts as an organization's linchpin for enterprise risk management (ERM), including IT and data security. CROs are fast becoming familiar faces among C-level executives at large organizations. According to Forrester Research Inc. in Cambridge, Mass., the executive ranks of any company that has revenue of at least $1 billion and can he classified as "critical infrastructure" — such as financial institutions, energy companies and health care providers — are likely to include a CRO. By next year, three quarters of large, critical infrastructure organizations will have a formal ERM office with a CRO or equivalent role, according to Forrester.

After its early emphasis in financial services, ERM has played an increasingly crucial part in business planning across industries during the past several years. Its widespread acceptance was spurred in part by regulations such as the Sarbanes-Oxley Act for accounting oversight and Basel II for measurement of international banking capital. As different types of operational risk also get included under the ERM umbrella, the CRO's job is to eliminate the "fragmented" approach to managing risk, according to Forrester.

With government regulations and the rise of corporate governance policies addressing enterprisewide risk, Forrester and other analyst firms have hammered on the importance of having a single point person in place to oversee its management.

"With the fragmented, siloed approach to risk management, there is no one watching risk across the organization," Forrester analyst Michael Rasmussen wrote in a December 2004 report on ERM trends. "In today's complex business world, one weak spot can impact the entire business. Without a framework to work within, and someone in charge of risk management, organizations are running in the dark."

An Expanding Role

One key to success for CROs is the ability to see the range of risk variations that can crop up across the enterprise. At The PMI Group Inc., a mortgage insurance company in Walnut Creek, Calif., the CRO position was created in 2003 to monitor international credit-risk operations. But the position's description has since heen expanded to encompass risk throughout the company, iocluding strategic, operational, external, financial, IT and security (both data and physical) operations.

"Without an enterprise view, things can he missed because you can't connect the risks," says Joanne Berkowitz, chief enterprise risk officer at PMI Group. "If you're just looking at your own little world and don't have an idea of how what you're doing will affect what someone else is doing, you could [inadvertently] create risk for the company."

In IT, Berkowitz says, disaster recovery illustrates this concept.

"We have very detailed business-resumption plans and capabilities. To create these, people in the business units worked closely with me and with our CIO to identify which systems they depend on and to prioritize their recovery times," she says. "This is particularly important because an increasing proportion of our business is automated; 90% of our business now comes through systems."

James Lam, president of James Lam & Associates loc., an enterprise risk consulting firm in Wellesley, Mass., agrees that the ability to see tbe big picture is key for the CRO.

"The key to success is having a strong background in the most critical risks to the company. You also have to look heyond your specific silo», across the enterprise, and have a comprehensive point of view," he says. "Organizations are realizing that a risk manager can help achieve a company's business objectives while he or she defends it from threats."

SOURCE: EXCLUSIVE COMPUTERWORLD SURVEY, MARCH 2006

An effective CRO has a range of skills that vary depending on the business focus, says Berkowitz. "There isn't just one set of skills that will work for a CRO, and they'll vary at each company," she says.

The position requires the ability to take a holistic view of the risks that might affect operations anywhere in the company. To that end, the CRO must work with other C-level executives, as well as with business unit managers, says Berkowitz.

"We're attempting to he proactive and to adopt good governance. Here, everyone would agree that the CRO is the person who's leading that effort," she adds.

With a CRO who takes a comprehensive view of risk across an organization, ERM can become a key piece of ao overall business plan.

Webster is a freelance writer in Providence, R.I. Contact him at john.s.webster@verizon.net.

Computer Forensics

DEFINITION

Computer forensics is the application of specialized investigative and analytic techniques to identify, collect, examine and preserve data from computer systems or networks so that it may serve as evidence in a court of law. More narrowly, the term applies to the process of finding digital evidence after a computer security incident has occurred.

BY RUSSELL KAY

THE TELEVISION series *CSI* has given millions of viewers an appreciation of the role and importance of physical evidence in conducting criminal investigations. Each week, we see the confluence of fingerprints, DNA tests, autopsies, microscopic examinations and ballistic evidence used to solve a murder or explain the circumstances surrounding an unusual death. The drama lies less in the events that are portrayed than in the thinking that lies behind the collection, preservation and interpretation of the evidence needed to solve the case and support prosecution.

IT managers aren't likely to confront dead bodies on the job, but a rudimentary knowledge of evidence, as it relates to computer data, can help protect your organization's operations, data and processes. In today's computer-driven world, where networked e-mail and instant messaging are the communication norms, knowing how to collect, handle and analyze information on a miscreant's computers can be critical to a successful civil or criminal prosecution.

QUICK STUDY

There are two categories of computer crime: criminal activity that involves using a computer to commit a crime, and criminal activity that has a computer as a target, such as a network intrusion or a denial-of-service attack.

The same means of gathering evidence are used to solve both types of crimes. And the same kinds of skills used by the lawbreakers are needed to track them down.

It Takes an Expert

Computer forensics is not a task to be undertaken lightly by just any IT worker. Instead, it calls for specialized skills and careful, documented procedures. A forensics expert knows what signs to look for and can identify additional information sources for relevant evidence, including earlier versions of data files or differently formatted versions of data used by other applications.

Computer data is fundamentally different in some respects from other types of information, and this affects how we have to handle it as evidence. Unlike a traditional paper trail, computer evidence frequently exists in many forms, and often different versions of documents are accessible on a computer disk or backup tapes.

Data stored on a computer or network is difficult to destroy completely, because the data is likely to coexist on multiple hard drives, and deleted files and even reformatted disks can often be fully recovered.

In addition, computer data can be replicated exactly for special analysis and processing without destroying the originals.

Any type of data can serve as evidence, including text documents, graphical images, calendar files, databases, spreadsheets, audio and video files, Web sites and application programs.

Even viruses, Trojan horses and spyware can be secured and investigated. E-mail records and instant messaging logs can be valuable sources of evidence in litigation, because people are often more casual when using electronic communications than they are when they use hard-copy correspondence such as written memos and snail-mail letters.

And finally, digital data can be searched quickly and easily by machine, whereas paper documents must be examined manually.

Like other information used in a case, however, the result of a computer forensics investigation must follow the accepted standards of evidence as codified in state and federal law.

In particular, an investigator must take special care to protect evidence and to preserve its original state. It's especially important to prevent suspect files from being altered or damaged through improper handling, viruses, electromagnetic or mechanical damage, and even booby traps. To accomplish this, it's necessary to do the following:

- Handle the original evidence as little as possible.
- Establish and maintain the chain of custody.
- Document everything that's done.
- Never go beyond what is known and can be proved from direct, personal knowledge.

Failure to protect evidence might mean that original data is irretrievably lost or changed and that results and conclusions may not hold up or be admissible in a court of law.

How It Works

While the circumstances of each case will differ, some elements are common to most computer forensic investigations. Here are some actions you should take:

- Secure the computer system to prevent it from being altered or tampered with by the investigators, third parties or automated processes such as viruses or other types of malware. Unless you can't avoid it, never analyze data using the machine it was collected from.
- Make exact, forensically sound copies of data storage devices, including all hard drives. Do not change date/time stamps or alter data itself. Do not overwrite unallocated space, which may happen when rebooting. Specialized equipment is available to speed and facilitate the forensic copying of hard drives.
- Identify and discover all files on the system, including normal files, deleted-yet-remaining files, hidden files, password-protected files and encrypted files.
- Recover deleted files as much as possible. Pay special attention to specific areas of the hard drive, including boot sectors, page files and temporary or swap files used by application programs and by the operating system.

Look at unallocated space (i.e., marked as currently unused), as well as the unoccupied space at the end of a file in the last assigned disk cluster after the end-of-file marker. Either area, though not considered a part of an active file, might hold relevant data from a different file or version of a document.

- Maintain a full audit log of your activities throughout the investigation, and produce a detailed report at the end. ●

COMPUTER FORENSICS is one aspect of a broader concept called electronic discovery, which refers to any process in which data from a particular computer or network is sought, located, secured and searched with the intent of using it as evidence in a civil or criminal legal case. Hacking that may be ordered by a court or sanctioned by a government agency to obtain evidence can also be considered a form of electronic discovery.

In general, discovery refers to the overall process, whereas computer forensics is concerned with specific procedures and technical interpretation of discovered data.

An important factor in electronic discovery is the completeness of information and the extent to which the organization may be required (by law or regulation) to maintain copies. When a party is required to supply documents and correspondence about a particular event or transaction, it is expected to provide all such documents without filtering or editing.

– RUSSELL KAY

Kay is a Computerworld contributing writer in Worcester, Mass. You can contact him at russkay@charter.net.

Are there technologies or issues you'd like to learn about in QuickStudy? Send your ideas to quickstudy@computerworld.com

To find a complete archive of our QuickStudies, go online to computerworld.com/quickstudies

Little Leaks

Flash drives, iPods, camera phones you know what your employees carry in. But do you know what they carry out?

By Steve Alexander

P[illegible]

But there can be huge consequences for IT departments that neglect the problem, Gold says. "Think about compliance issues if an insurance company employee downloads a couple of thousand customer records onto a flash drive and then loses the device," he says. "And often, the company won't even know the employee has done it." The result can be lawsuits and, if federal medical or financial privacy rules have been violated, multimillion-dollar fines, according to Gold.

The payback for doing a good job with security for these personal devices is preventing a $10 million to $50 million company liability, Gold says.

Data Guardians

While relatively few companies are addressing the issue, some have tried solutions ranging from total network lockdowns to requiring the use of encrypted flash drives to ensure that data will at least be safeguarded if it is lost.

At the less restrictive end of the spectrum is Children's Home Society of Florida (CHS), an adoption and family counseling agency in Winter Park.

"We deal with private medical information, and it's been a long-standing problem," said CIO John Valleau. "Our employees have floppy disks, flash drives and iPods to which information can be transferred."

As a result, CHS has [illegible]

[illegible]

encrypted flash drives at the 1,000 computer workstations at the firm's 210 offices around Florida.

Hospitals, which must closely guard patient information under the Health Insurance Portability and Accountability Act, are particularly concerned about flash drives.

"While personal storage devices haven't been a big problem for us, we need to be able to prove that we are protecting patient information," says Mark McCall, a network engineer who administers security for 900 workstations and 1,200 users at Ellis Hospital in Schenectady, N.Y.

"Many people have access to patients' Social Security numbers, personal information and diagnoses. So we toyed with banning flash drives and camera phones — a double threat when the camera phones contain memory cards that can hold data — but some people have a valid use for them," he explains. "And when we started to lock things down, the users screamed. One doctor said he couldn't give his PowerPoint presentation at another hospital."

McCall's solution was to install Sanctuary, a network monitoring product from SecureWave SA in Luxembourg that can restrict the use of personal storage devices based on a user's identity, individual PC workstations or the type of personal data device being connected to the network. Exceptions can be made for reasonable data-access requests, he says. However, the software can't protect against the use of a camera phone not connected to the network, so the hospital relies on a policy limiting where photos can be taken.

Network Lockdown

A more extreme approach was taken by Fabi Gower, vice president of information systems at Martin, Fletcher & Associates LP. The national health care staffing firm in Irving, Texas, has databases containing proprietary information about job candidates. Gower uses network-control software to limit both the type of content users can view and the time of day they can see it. Her company totally prohibits employees other than managers from copying data by limiting the network's ability to write to portable storage devices.

"I'm a strong proponent of having control over the security of the business, whether you've got two employees or 2,000," Gower says. "The way we've got the network set up, employees can't plug PDAs, smart phones, flash drives or USB hard drives into the network. So I couldn't care less what they carry in, because I know our data is not leaving the building."

But some company's data will get out, Gold predicts. "I have no doubt that, with all these portable memory devices in the workplace, there will be a federal privacy compliance breach in the next year. And it could be a huge liability." ■

Alexander is a freelance writer in Edina, Minn. Contact him at s[illegible]alexander@rocketmail.com.

Does your company have a policy that bans or limits the use of [illegible] following devices at work?

Yes, camera phones

Yes, USB flash drives or other portable storage media

None of the above is limited or banned

Other

BASE: 571 IT professionals; respondents could choose all that apply

How to Stop the Leaks

FIRST LINE OF DEFENSE: [illegible]

SECOND LINE OF DEFENSE: [illegible]

[illegible] practical because too many legitimate [illegible] use them. Another alternative is [illegible] employees encrypted flash drives to protect the data in case the tiny device [illegible] lost.

THIRD LINE OF DEFENSE: [illegible] employees [illegible] the portable [illegible]

Little Leaks

Flash drives, iPods, camera phones — you know what your employees carry in. But do you know what they carry out?

By Steve Alexander

PROLIFERATING FLASH drives and other personal memory devices are causing corporate IT managers to rethink data security policies and enforcement. But the balance between corporate security and user convenience has never been more difficult to achieve, because ubiquitous thumb-size drives can hold gigabytes of corporate information.

"In many cases, it's an unrecognized security problem," says Jack Gold, founder of J. Gold Associates, an IT consulting firm in Northboro, Mass. "And it's not just flash drives. A lot of users have discovered that iPods make convenient backup devices."

But there can be huge consequences for IT departments that neglect the problem, Gold says. "Think about compliance issues if an insurance company employee downloads a couple of thousand customer records onto a flash drive and then loses the device," he says. "And often, the company won't even know the employee has done it." The result can be lawsuits and, if federal medical or financial privacy rules have been violated, multimillion-dollar fines, according to Gold.

"The payback for doing a good job with security for these personal devices is preventing a $10 million to $30 million company liability," Gold says.

Data Guardians

While relatively few companies are addressing the issue, some have tried solutions ranging from total network lockdowns to requiring the use of encrypted flash drives to ensure that data will at least be safeguarded if it is lost.

At the less restrictive end of the spectrum is Children's Home Society of Florida (CHS), an adoption and family counseling agency in Winter Park.

"We deal with private medical information, and so it's been a long-standing problem," said CIO John Valleau. "Our employees have floppy disks, flash drives and iPods to which information can be transferred."

Although CHS has a "thou shalt not copy" policy regarding the downloading of sensitive information to portable memory devices, Valleau says he isn't about to ban them, because "some people might need to carry protected medical records from one location of ours to another."

As a result, Valleau is looking at requiring employees to use only new, encrypted flash drives at the 1,000 computer workstations at the firm's 210 offices around Florida.

Hospitals, which must closely guard patient information under the Health Insurance Portability and Accountability Act, are particularly concerned about flash drives.

"While personal storage devices haven't been a big problem for us, we need to be able to prove that we are protecting patient information," says Mark McGill, a network engineer who administers security for 900 workstations and 1,200 users at Ellis Hospital in Schenectady, N.Y.

"Many people have access to patients' Social Security numbers, personal information and diagnoses. So we toyed with banning flash drives and camera phones — a double threat when the camera phones contain memory cards that can hold data — but some people have a valid use for them," he explains. "And when we started to lock things down, the users screamed. One doctor said he couldn't give his PowerPoint presentation at another hospital."

McGill's solution was to install Sanctuary, a network monitoring product from SecureWave SA in Luxembourg that can restrict the use of personal storage devices based on a user's identity, individual PC workstations or the type of personal data device being connected to the network. Exceptions can be made for reasonable data-access requests, he says. However, the software can't protect against the use of a camera phone not connected to the network, so the hospital relies on a policy limiting where photos can be taken.

Network Lockdown

A more extreme approach was taken by Fabi Gower, vice president of information systems at Martin, Fletcher & Associates LP. The national health care staffing firm in Irving, Texas, has databases containing proprietary information about job candidates. Gower uses network-control software to limit both the type of content users can view and the time of day they can see it. Her company totally prohibits employees other than managers from copying data by limiting the network's ability to write to portable storage devices.

SOURCE: EXCLUSIVE COMPUTERWORLD SURVEY, MARCH 2006

"I'm a strong proponent of having control over the security of the business, whether you've got two employees or 2,000," Gower says. "The way we've got the network set up, employees can't plug PDAs, smart phones, flash drives or USB hard drives into the network. So I couldn't care less what they carry in, because I know our data is not leaving the building."

But some company's data will get out, Gold predicts. "I have no doubt that, with all these portable memory devices in the workplace, there will be a federal privacy compliance breach in the next year. And it could be a huge liability."

Alexander is a freelance writer in Edina, Minn. Contact him at s_j_alexander@rocketmail.com.

How to Stop the Leaks

FIRST LINE OF DEFENSE: Establish a portable-device policy and educate users about it. Few companies ban the devices outright: 15% to 20% have usage polices.

SECOND LINE OF DEFENSE: Implement network safeguards. Network management tools, used by less than 5% of corporations, can restrict network access by individual, workstation or type of device. Shutting down all USB ports isn't practical because too many legitimate devices use them. Another alternative is to issue employees encrypted flash drives to protect the data in case the tiny devices get lost.

THIRD LINE OF DEFENSE: Dismiss employees caught violating the portable-device rules. This can help you avoid potentially huge corporate liabilities for compromises of confidential data.

SOURCE: J. GOLD ASSOCIATES, NORTHBORO, MASS.

Snapshots

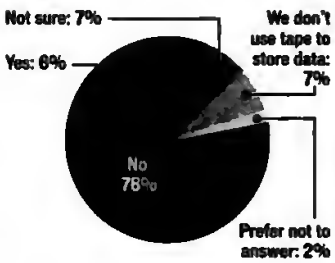
Who's in Charge?

A ranking of the departments involved in setting IT security spending priorities

1. IT only
2. Finance and IT
3. Top executives (CEO, COO)
4. IT steering committee
5. All departments, to some degree
6. Managers of business units
7. Risk management committee
8. Finance only

Caught on Tape

If your company uses tape storage, in the past year have tapes been lost, stolen or misplaced?



Security Arsenal

Top security products or services currently being used.

1. Desktop antivirus software
2. Antivirus software
3. Enterprise firewalls (appliances)
4. Antispyware software
5. IPsec virtual private networks
6. URL blocking and filtering
7. Network intrusion detection
8. Enterprise firewalls (software)
9. Desktop firewalls
10. Network intrusion prevention
11. E-mail encryption software
12. Desktop/laptop/handheld file-encryption software

Base: 571 IT professionals

SOURCE: EXCLUSIVE COMPUTERWORLD SURVEY MARCH 2006

MARK HALL

No Silver Bullet

FIRST, THE BAD NEWS. THEN, THE WORSE NEWS. We are years away from having a single security architecture to protect company information. That's because every area in IT has different technical hurdles to cross before security can be assured. And in each segment today, we are a long way from satisfactory protection.

Evalubase Research Inc. released a survey in February that covered five technology areas: data management, hardware and operating systems, communications and networking, application development, and industry applications. The research firm asked IT professionals to rank those technologies for performance, usability, functionality, compatibility, maintainability and security. You won't be shocked to learn that security ranked at the bottom for all except hardware and operating systems, and communications and networking, where it was ranked next to last.

Nick Caffarra, president of Evalubase, tells me that maybe, *maybe*, in five or more years there could be an integrated cross-technology security approach from one vendor capable of protecting your information. But he doesn't sound optimistic.

Little wonder that he isn't bullish on a single security approach, because here's the worse news. It comes from Seth Hallem, CEO of Coverity Inc. His company scans source code for defects, most of which lead to security holes. (The Department of Homeland Security and Stanford University chose Coverity to analyze open-source tools for defects.) Hallem points to research that proves it's mathematically impossible to eliminate defects from source code. Mathematically impossible.

So, that's the news. Your company's information isn't secure today, and it won't ever be.

It's All Relative

Of course, security is relative. Last month, the folks at Coverity released some data for defect scans on 31 open-source projects. The average defect rate for 1,000 lines of source code was 0.42. Not bad. A programmer would, on average, crank out 2,200 lines of code for each flub. But if that rate were constant against, say, the 30 million lines of Red Hat Linux 7.1, you'd have 12,600 lines with problems. If it held steady against the 213 million lines of source in Debian 3.1, you'd find 89,460 potential defects.

This isn't to say that Debian is less secure as a server operating system than Red Hat. Or vice versa. But it does point to the kind of information you can use to lower the risk your information faces. That is, you can use tools to quantify your risk and then decide when, where and whether to use a technology.

Common Sense

You can also use common-sense strategies to protect your company's information. Would your data be inherently more secure if more end users had Macintoshes? Despite news in February that the first (benign) virus for the Mac was discovered, the answer would have to be yes. That's because viruses and worms written for one system wouldn't be propagated by the other. In other words, a mix of operating systems is a good defensive strategy.

Do all end users really need fat clients — Windows or Macs? Would some be able to get their work done more securely on thin clients? Of course.

A mix of thin clients, Macs and Windows, as well as different server systems, is an ideal defense against many of today's vulnerabilities. A side benefit is challenging the skills of hackers who will try to penetrate your defenses with primarily Windows-specific knowledge.

Some single-platform advocates argue that the IT costs of running multiple operating systems make it problematic to run a mixed environment. Maybe so. But these people have a short-term view of cost. The costs of a security breach are far greater. The University of Maryland estimates that when a public company suffers a single security breach, its market capitalization drops 5%. Would you want to tell the board of directors not to worry because the company saved some of that shareholder value in IT support costs through your single-platform strategy?

Business = Risk

Every business faces risk the moment it opens its doors. IT's job is to keep the risk to information at a minimum. Hoping for one solution — the security silver bullet — isn't realistic. The one-way approach has proved to be a security liability when implemented as a uniform platform strategy.

Given how valuable information is to a company, Evalubase's Caffarra says it might be time to put corporate data on a company's balance sheet as an asset. If that happened, maybe the board would insist that the very best tools and methodologies be applied to decrease the risk to that information. And that the very best strategy isn't to put all your eggs in one basket.

COMPUTERWORLD HEADQUARTERS

One Speen Street P.O. Box 9171
Framingham, MA 01701-9171
Phone: (508) 879-0700
Fax: (508) 875-4394

PRESIDENT/PUBLISHER/CEO
Matthew J. Sweeney
(508) 271-7100

EXECUTIVE ASSISTANT TO CEO/ CORPORATE COMMUNICATIONS MANAGER
Laureen Austermann
(508) 820-8522

VICE PRESIDENT/ GENERAL MANAGER ONLINE
Martha Connors
(508) 620-7700

VICE PRESIDENT/MARKETING
Matt Duffy
(508) 820-8145

DIRECTOR/ HUMAN RESOURCES
Julie Lynch
(508) 820-8162

EXECUTIVE VICE PRESIDENT/ STRATEGIC PROGRAMS
Ronald L. Milton
(508) 820-8661

VICE PRESIDENT/ONLINE SALES
Gregg Pinsky
(508) 271-8013

EXECUTIVE VICE PRESIDENT/COO
Matthew C. Smith
(508) 820-8102

VICE PRESIDENT/ EDITOR IN CHIEF
Don Tennant
(508) 620-7714

VICE PRESIDENT/CIRCULATION
Debbie Winders
(508) 820-8193

CIRCULATION
Sr. Circulation Specialist/Diana Tasco, (508) 820-8167

PRODUCTION
Vice President Production/Carolyn Medeiros. Production Manager/Kim Pennett. Print Display Advertising: (508) 820-8232. Fax: (508) 879-0446. DISTRIBUTION: Director of Distribution and Postal Affairs/Bob Wescott

STRATEGIC PROGRAMS AND EVENTS
Vice President Strategic Initiatives/Leo Leger. Vice President Business Development/John Amato. Senior Director Event Sponsorship Sales/Ellen Harris. Vice President, Event Marketing and Conference Programs/Derek Hulitzky. Director, Event Management/Michael Maloney. Program Director, Computerworld Honors/Sandy Weill. Business Development Specialist/Colin Longual. Business Development Specialist/Chris Legeir. Business Development Specialist/Amy McLellan. Marketing Manager/Timothy Johnson. Conference Manager/Nancy Feldsham. Sr. Marketing Specialist/Duncan Newell. Executive Programs Specialist-Computerworld Honors/Deborah Lee. Executive Programs Specialist-Executive Assistant/ Kelly McGill. Custom Events Specialist/Jean Lee. Operations Specialist/Chris Johnson. Web Development Specialist/Michelle Ramsey. Customer Service Coordinator/Josh Ryan. Audience Development Coordinator/Shan Ebb. One Speen Street, Box 9171, Framingham, MA 01701-9171, (508) 879-0700. Fax: (508) 626-8524

ONLINE ADVERTISING
Director of Online Sales/Sean Weglage, (415) 978-3314, Fax: (415) 543-8010. Online Sales Manager, East Coast/James Kalbach, (610) 971-1588. Online Account Executive/April Hughes, (415) 978-3311, Fax: (415) 543-8010. Online Account Executive/Matthew Wimmingham, (508) 270-3682. Fax: (508) 270-3882. Senior Account Services Manager/Bill Rigby, (508) 620-8111, Fax: (508) 270-3882. Online Account Services Specialist/Kathryn Grey, (508) 620-7760. Fax: (508) 270-3882. Online Sales Assistant/Kathy Snow (508) 270-7112. One Speen Street, Box 9171, Framingham, MA 01701-9171, Fax: (508) 270-3882.

IT CAREERS ADVERTISING SALES OFFICE
Director of Sales/Laura Wilkinson, (847) 441-8677. Fax: (847) 441-8878. One Speen Street, Framingham, MA 01701

LIST RENTAL
POSTAL: Rob Green, (508) 370-0832, e-mail: rgreen@idglist.com. E-Mail: Christine Cahill, (508) 370-0808, e-mail: ccahill@idglist.com. MAILING ADDRESS: IDG List Services, P.O. Box 9151, Framingham, MA 01701-9151. Fax: (508) 370-0020

COMPUTERWORLD SALES OFFICES

PRESIDENT/PUBLISHER/CEO
Matthew J. Sweeney
(508) 271-7100
Fax: (508) 270-3882

SALES INTEGRATION DIRECTOR
Laurie Marinone
(508) 628-4823
Fax: (508) 270-3882

NORTHWESTERN STATES
ACCOUNT DIRECTOR: Jim Barrett (415) 978-3306
ACCOUNT EXECUTIVE: Chris Da Rosa (415) 978-3304, 501 Second Street, Suite 114, San Francisco, CA 94107. Fax: (415) 543-8010

BAY AREA
ACCOUNT DIRECTORS: Jim Barrett (415) 978-3306, Sara Culley (415) 978-3307. ACCOUNT EXECUTIVES: Chris Da Rosa (415) 978-3304, Emmie Hung (415) 978-3308, 501 Second Street, Suite 114, San Francisco, CA 94107. Fax: (415) 543-8010

SOUTHWESTERN STATES
ACCOUNT DIRECTOR: Bill Hanck (949) 442-4006
ACCOUNT EXECUTIVE: Jean Dellarobba (949) 442-4053, 19200 Von Karman Avenue, Suite 360, Irvine, CA 92612. Fax: (949) 476-8724

EASTERN CENTRAL STATES/INDIANA
ACCOUNT DIRECTOR: Peter Mayer (201) 634-2324
ACCOUNT EXECUTIVE: John Radzniak (201) 634-2323, 650 From Road · 2nd Floor, Paramus, NJ 07652. Fax: (201) 634-9289

CENTRAL STATES
ACCOUNT DIRECTOR: Bill Hanck (949) 442-4006
ACCOUNT EXECUTIVE: Jean Dellarobba (949) 442-4053, 19200 Von Karman Avenue, Suite 360, Irvine, CA 92612. Fax: (949) 476-8724

NEW ENGLAND STATES
ACCOUNT MANAGER: Deborah Crimmings (508) 271-7110. SALES ASSOCIATE: Jess Roman (508) 271-7108, One Speen Street, Framingham, MA 01701. Fax: (508) 270-3882

METRO NEW YORK
ACCOUNT DIRECTOR: Peter Mayer (201) 634-2324
ACCOUNT EXECUTIVE: John Radzniak (201) 634-2323, 650 From Road · 2nd Floor, Paramus, NJ 07652. Fax: (201) 634-9289

SOUTHEASTERN STATES
ACCOUNT DIRECTOR: Lisa Ladle-Wallace (904) 284-4972, 5242 River Park Villas Dr., St. Augustine, FL 32092. Fax: (800) 779-8622. SALES ASSOCIATE: Jess Roman (508) 271-7108, One Speen Street, Framingham, MA 01701. Fax: (508) 270-3882

ADVERTISER'S INDEX

*Regional Select Edition

This index is provided as an additional service. The publisher does not assume any liability for errors or omissions.

INTERNATIONAL DATA GROUP

CHAIRMAN OF THE BOARD
Patrick J. McGovern

PRESIDENT, IDG COMMUNICATIONS
Bob Carrigan

COMPUTERWORLD is a business unit of IDG, the world's leading technology media, research and event company. IDG publishes more than 300 magazines and newspapers and offers online users the largest network of technology-specific sites around the world through IDG.net (www.idg.net), which comprises more than 330 targeted Web sites in 80 countries. IDG is also a leading producer of 168 computer-related events worldwide, and IDG's research company, IDC, provides global market intelligence and advice through 51 offices in 43 countries. Company information is available at www.idg.com.

IDG

Have a problem with your Computerworld subscription?

We want to solve it to your complete satisfaction, and we want to do it fast. Please write to **Computerworld, P.O. Box 3500, Northbrook, IL 60065-3500.**

Your magazine subscription label is a valuable source of information for you and us. You can help us by attaching your magazine label here, or copy your name, address, and coded line as it appears on your label. Send this along with your correspondence.

ADDRESS CHANGES OR OTHER CHANGES TO YOUR SUBSCRIPTION
All address changes, title changes, etc. should be accompanied by your address label, if possible, or by a copy of the information that appears on the label, including the coded line.

YOUR NEW ADDRESS GOES HERE: **ADDRESS SHOWN:** ❑ Home ❑ Business

NAME
TITLE COMPANY
ADDRESS
CITY STATE ZIP

OTHER QUESTIONS AND PROBLEMS
It is better to write us concerning your problem and include the magazine label. Also, address changes are handled more efficiently by mail. However, should you need to reach us quickly, the following toll-free number is available. **(888) 559-7327 Outside U.S. call (847) 559-7322.**
Internet address: cw@omeda.com

COMPUTERWORLD allows advertisers and other companies to use the mailing list for selected offers we feel would be of interest to you. We screen these offers carefully. If you do not want to remain on the promotion list, please write to the following address – COMPUTERWORLD, Circulation Department, One Speen Street, Framingham, MA 01701.

NAME
TITLE COMPANY
ADDRESS
CITY

HOW TO CONTACT COMPUTERWORLD

We invite readers to call or write with their comments and ideas. It is best to submit ideas to one of the department editors and the appropriate beat reporter.

Don Tennant (508) 620-7714
Editor in chief

Mitch Betts (301) 262-8243
Executive editor

Julia King (610) 532-7599
Executive editor, events

DEPARTMENT EDITORS

Craig Stedman (508) 820-8120
News editor

Mike Bucken (508) 820-8562
Assistant News editor

Tommy Peterson (508) 620-7729
Technology editor

Kathleen Melymuka (508) 820-8118
Management editor

REPORTERS

Sharon Fisher (508) 879-0700
Storage: disaster recovery/business continuity

Matt Hamblen (508) 820-8567
Networking: mobile/wireless, network/systems management

Heather Havenstein (919) 386-0381
Business intelligence; application development, Web services, application server software; health care industry

Eric Lai (510) 768-2818
Windows, Linux, desktop applications, databases, financial services industry

Linda Rosencrance (508) 628-4734
General assignment: transportation and automotive industries

Carol Sliwa (508) 628-4731
National correspondent

Marc L. Songini (508) 820-8182
ERP, supply chain and CRM applications; RFID, retail, food and agribusiness industries

Patrick Thibodeau (202) 333-2448
Enterprise systems, Unix, outsourcing and immigration, antitrust issues

Jaikumar Vijayan (630) 978-8390
Corporate security/privacy issues, related legislation and regulations

Todd R. Weiss (717) 560-5255
General assignment: open-source community, intellectual property: messaging/collaboration

FEATURES

Ellen Fanning (508) 820-8204
Special projects editor

Thomas Hoffman (845) 988-9630
National correspondent

Robert L. Mitchell (508) 820-8177
National correspondent

Mark Hall (503) 391-1158
Editor at large

Gary H. Anthes (703) 536-9233
National correspondent

Julia King (610) 532-7599
National correspondent

OPINIONS

Frank Hayes (503) 252-0100
Senior news columnist

COMPUTERWORLD.COM

Martha Connors (508) 620-7700
Vice president/general manager

Scot Finnie (508) 628-4868
Online editorial director

Ian Lamont (508) 820-8187
Senior online projects editor

Gregg Linde (508) 820-8217
Online production manager

Joyce Carpenter (508) 820-8161
Online projects editor

Sharon Machlis (508) 820-8231
Managing editor/online

Ken Mingis (508) 820-8545
Online news editor

Marian Prokop (508) 620-7717
Online editor at large/Networking channel editor

David Ramel (508) 820-8269
E-mail newsletters/Networking channel editor

Lucas Mearian (508) 820-8215
Storage channel editor

Angela Gunn (206) 388-2508
Security channel editor

John R. Brillon (508) 820-8216
Associate art director

Dawn Petersen (508) 820-8131
Production designer

Susan Cahill (508) 271-7122
Associate online production designer

Peter Smith
Web development manager

Kevin Gerich, Mark Savery
Web developers

RESEARCH

Mari Keefe
Research manager

Gussie Wilson
Research associate

COPY DESK

Michele Lee DeFilippo (508) 820-8126
Managing editor/production

Bob Rawson (508) 271-8015
Assistant managing editor/production

Eugene Demaitre, Monica Sambataro
Senior copy editors

Donna Sussman
Copy editor

GRAPHIC DESIGN

Stephanie Faucher (508) 820-8235
Design director

April O'Connor
Art director

Owen Edwards
Associate art director

ADMINISTRATIVE SUPPORT

Linda Gorgone (508) 820-8176
Office manager

CONTRIBUTING EDITOR

Jamie Eckle (617) 596-1673
Opinions

CONTRIBUTING COLUMNISTS

Michael Gartenberg, Paul Glen, Barbara Gomolski, John Halamka, Thornton A. May, David Moschella, Bart Perkins, Virginia Robbins, Bruce A. Stewart

CONTRIBUTING WRITERS

Mary Brandel, Stacy Collett, Russell Kay, Mary K. Pratt, Drew Robb

TELEPHONE/FAX
Main phone number (508) 879-0700
All editors unless otherwise noted below
Main fax number (508) 875-8931
24-hour news tip line (508) 620-7716

E-MAIL
■ Our Web address is www.computerworld.com.
■ Staff members' e-mail follows this form: firstname_lastname@computerworld.com.
■ For IDG News Service correspondents: firstname_lastname@idg.com.

LETTERS TO THE EDITOR
Letters to the editor are welcome and should be sent to: letters@computerworld.com. Include your address and telephone number.

MAIL ADDRESS
PO Box 9171, 1 Speen Street, Framingham, Mass. 01701

SUBSCRIPTIONS/BACK ISSUES
Subscription rates:
■ U.S., $99.99/year
■ Canada, $130/year
■ Central and South America, $250/year
■ All others, $295/year
Phone (888) 559-7327
E-mail cw@omeda.com
Back issues (888) 559-7327

REPRINTS/PERMISSIONS
Contact Erik Eberz
Phone (717) 399-1900, ext. 150
E-mail computerworld@reprintbuyer.com
Visit www.reprintbuyer.com to obtain quotes and order reprints online.

COMPANIES IN THIS ISSUE

Page number refers to page on which story begins. Company names can also be searched at www.computerworld.com

Continued from page 1

Bird Flu

CIOs said the possibility of a major flu outbreak isn't that big of concern for them, despite warnings dating back to early last year from the federal government, international groups and consulting firms such as Gartner Inc.

says his company is brainstorming various disaster scenarios.

"I don't view [pandemic preparations] as that important," said Amy Fowler, president of the Colorado chapter of the Society for Information Management and an IT management consultant to large companies. "What are the odds of [a long quarantine] happening? We have bigger issues in IT than that one."

Dave Berg, CIO at O.C. Tanner Co., a provider of employee-recognition products and services in Salt Lake City, also hasn't made planning for a possible flu outbreak an action item. Berg noted that most of his employees have secure, high-speed computer access at home and that most operations can be done remotely. "I do not think we would have a serious problem here with keeping our computers and applications services available," he said.

Gartner has issued several advisories about a possible pandemic, urging IT shops to prepare for the need to upgrade broadband and virtual private network connections to the homes of key workers and beef up their online ordering capabilities for customers.

In a 31-page report issued March 7, the consulting firm listed in stark detail three scenarios for a global spread of the avian flu or another virus, from mild to severe. In the most severe scenario, several million people would die and the pandemic could last for a year or longer, despite strict quarantines. Many businesses would cease to operate, travel would be restricted, and workplace communications would often be done via phone, videoconferencing and e-mail.

But Gartner analyst Ken McGee last week rated overall corporate preparation levels at only a 2 or 3 on a scale from 1 to 10. "Maybe pandemic planning isn't the most important thing facing a company, but it should be in the top two," McGee said, suggesting that tight IT budgets might be keeping some companies from moving more quickly to prepare.

The biggest mistake companies are making is assuming that their existing continuity plans will work in the event of a pandemic, McGee added. "Unlike earthquakes and hurricanes and bombs, which are geographically confined, a pandemic is not," he said. "At Gartner, we can't comprehend what IT is thinking on this, because a pandemic is the gift that keeps on giving."

Kevin Desouza, an assistant professor at the University of Washington's Information School in Seattle, said he knows of "only a very few companies" that have systematic plans for monitoring whether a crisis is coming and for responding before a pandemic hits.

"The chief complaint of CIOs is that they walk a fine line between saying, 'The sky is falling' and educating people [about] the inherent risks associated with a pandemic crisis," he said.

Small and midsize businesses in particular are "way down the list" in terms of preparedness, Desouza added.

Some IT managers said they're working to adapt their companies' business continuity plans to a potentially widespread and long-duration pandemic. "In a pandemic, people would have to stay at home to prevent the spread of whatever the virus is, so we need to find ways to [support] that," said Ellen Barry, CIO at the Metropolitan Pier and Exposition Authority in Chicago and president of that city's local SIM chapter.

For example, to limit the amount of data traffic that moves across network pipes, Barry is considering putting the bulk of the authority's applications on centralized servers, following the concept behind WAN optimization products from vendors such as Citrix Systems Inc.

Barry said she has been planning for a pandemic for six months and recently attended two conferences where the topic was addressed.

Another potential problem, Barry said, is that even if workers have appropriate broadband connectivity and good PCs to use at home, they probably won't be as productive as usual if they are sick or involved in caring for someone who is ill.

Just in Case

Lawrence Robert, director of business continuity at a large financial services firm based in New England, said his company, which he asked not be named, has begun expanding its planning processes to include a possible pandemic.

The company is brainstorming disaster scenarios internally and sending detailed questionnaires to its telecommunications carriers seeking assurances that they will be able to handle network loads in residential areas efficiently and securely if a pandemic occurs, said Robert, who is a director of the 1,200-member New England Disaster Recovery Information X-change.

Some carriers have said that if broadband customers who need to work from home sign up in advance of a pandemic, there should be enough network capacity in the event of quarantines.

But "that's not necessarily true," Robert said. His company is taking into consideration the distances between the homes of critical workers and the central offices of their broadband providers. One goal of the ongoing research is to help company officials decide how many more laptops and VPNs need to be deployed.

Robert doesn't care whether the odds of a pandemic occurring are low or high. "Business continuity planners don't look at cause so much as effect," he said. "So whether there's a fire or a bomb or a pandemic, [if] the building is out, the workforce has to be disseminated." The biggest difference might be that the period of disruption could last longer during a pandemic than it would during another event, he added.

However, Desouza noted that a pandemic could produce "things that we did not predict, which can combine to cause problems we didn't imagine." ■

Prep Work

What IT managers should do to prepare for a possible avian flu pandemic:

- Make your workforce aware of the threat and what you're doing to prepare for it.
- Establish or broaden work-at-home policies that include the use of broadband services, appropriate security and network access to applications.
- Expand online transaction-processing and self-service options for customers and business partners.
- Invest in videoconferencing technology to use if travel restrictions are imposed.
- Work with customers and partners to minimize disruptions by coordinating crisis-response capabilities.

IT Staffing Issues Play a Role in Pandemic Planning

PREPARATIONS FOR an avian flu pandemic are extending beyond IT infrastructure and network issues to staffing considerations, including what to do if critical workers die or if a business temporarily closes and then needs to staff up again when it reopens.

Ellen Barry, CIO at the Metropolitan Pier and Exposition Authority in Chicago, said her organization's conference facilities would probably close during a pandemic, but staffers would need to remain on the payroll and be able to communicate with one another and with customers to plan future shows. A similar situation occurred when business travel slowed after the 9/11 terrorist attacks, Barry said.

Andy Wihtol, founder of Andrew Associates Executive Search in Lake Oswego, Ore., said IT organizations need to "think about having a bench, like a farm league in baseball." Companies should have not only in-house successors ready to step in for missing workers but also potential outside replacements for critical positions, Wihtol said. "You identify two to three people who [could] come in if a key person left or died, and then stay in touch with them," he said.

Kevin Desouza, an assistant professor at the University of Washington's Information School in Seattle, said some large companies are dealing with the possible loss of critical workers by cross-training IT staffers in different jobs and skills. "That way, if somebody goes, the new worker doesn't have to learn everything from scratch," Desouza said.

He added that if a pandemic occurs and IT workers are left idle because business productivity is down, it could be a good time for them to do home-based training or work on new technologies that might have been shelved previously. "You need to keep workers engaged," he said.

– MATT HAMBLEN

[illegible] CANADIAN POSTMASTER: [illegible] POSTMASTER: [illegible]

FRANK HAYES ■ FRANKLY SPEAKING

Routed by Rootkits

CALL it the worst work-around ever. How else to describe the advice from Mike Danseglio, a Microsoft security guru, to wipe and reinstall Windows on any PC infected with an insidious malware known as a rootkit? Danseglio grabbed some headlines this month when he told an audience at the InfoSec World security conference that once a rootkit digs in, there's no sure way to get rid of it short of nuking Windows and starting from scratch.

But it turns out his suggestion isn't new. Danseglio's been giving that advice for most of a year. He wrote a Microsoft "Security Tip of the Month" that said the same thing last October.

And it's good advice. But as a work-around, it's terrible.

It's good advice because Danseglio's probably right: There's no other way to root out a rootkit. We can try to *prevent* infections — with firewalls, virus scanners, software patches and updates. But once a rootkit is in, it's in. It spreads its hooks everywhere. Rootkits are like cancer. You can cut out the obvious tumor, but there's no way to be absolutely sure you've removed every malignant cell from a patient's body.

We can't eliminate biological cancers with a wipe and reinstall. But we can get rid of rootkits that way. And if there's nothing better, it's a realistic tactical approach to the problem.

But it's still an awful work-around. Why? Because a work-around should be a trade-off, a rational decision about how to use resources. Work-arounds make sense when they cost less than fixing underlying problems. But a work-around's cost piles up over time. Eventually you *do* want those underlying problems fixed.

In Windows, that's not going to happen. The rootkit vulnerabilities go to the core of Windows. They're not just bugs; they're flaws in Windows' basic design. Waiting for Microsoft to fix them is pointless. Microsoft doesn't have a fix, at least not short of entirely ripping out and replacing the guts of Windows.

And the only trade-off is that we foot the bill for Microsoft's years of failure to secure Windows.

Yes, some rootkits will be blocked by tighter security in Vista when it finally arrives — but not all rootkits. The soonest we can hope for a completely rearchitected, rootkit-proof Windows is literally years from now. And Microsoft has yet to promise anything like that.

FRANK HAYES, *Computerworld's* senior news columnist, has covered IT for more than 20 years. Contact him at frank_hayes@computerworld.com.

Meanwhile, we don't have just one work-around for the rootkit problem. We can actually try three different approaches.

Option A: Nuke and restore. You can automate the process. It might even become smooth — for IT. But don't underestimate the cost in lost productivity for users, who'll still have to adjust settings, rebuild their desktops and shortcuts, and reinstall their own applications (yes, they have them, even if they don't tell IT about them).

Option B: Change your Windows architecture. You can run Windows applications from a terminal server like Citrix. Or virtualize them with Softricity. Or move everything to blades. Yeah, it's a pricey transition, and it'll shake up users. You'll also probably need a lot more network bandwidth. But rebuilding all those PCs will be easier if it's ever necessary.

Option C: Abandon Windows. Whether that means Web-based apps or Linux or Macs or terminals, it's likely to be the most disruptive and costly option in the short term for both users and IT, and it will radically change what your IT shop does.

None of those options is a true trade-off. The cost and effort is all ours. We're facing complex and expensive choices, with no certainty that we'll ever see the underlying flaws fixed. Right now, it's all Microsoft can do to fix surface-level problems like buffer overflows.

It's going to require a completely new Windows core to finally purge the rootkit cancer for good. And that's going to take a very hard, very expensive decision by Microsoft.

Not just the worst of work-arounds for us. ▸

What the @#$%! Is Wrong?

Spam filter catches an outgoing e-mail message with language that would make a sailor blush, and IT pilot fish forwards it to HR, as required by company policy. Turns out there's an explanation – sort of. "The employee said his home e-mail wasn't working, or so he thought," says fish. "So he drafted an expletive-filled missive at work and sent it to his home e-mail account. Not receiving it, he concluded that his home e-mail wasn't working and contacted his ISP. There really is no cure for stupid."

SHARK TANK

Aha!

Remote office can't access the system at headquarters one day, so HQ pilot fish tests the remote equipment. "Neither the router nor the CSU/DSU, which connects the office LAN to the dedicated circuit, could be looped," says fish, who calls the phone company. Several hours later, telco calls back with the answer: "The smartjack, CSU/DSU, router, dumb terminal and printer were all gone," sighs fish. "Everything had been stolen."

Useless

User's personal mouse won't work with her laptop, and she demands that pilot fish fix it right away. "She said, 'Look, the laptop is not getting the information from the mouse,' " says fish. "I asked where the receiver to the wireless mouse was. She looked at me like I was an idiot. 'Isn't this a wireless laptop? Here's my wireless mouse. They should go together.' Again, I asked where the what-a-ma-thing with the black cable was. 'I got rid of the extra stuff,' says user. 'It wasn't needed.' "

One Step At a Time

State agency spends $100,000 to install high-speed Internet connections so local governments can file reports with the agency electronically, reports a pilot fish in the mix. "Finally, they send out an e-mail with an attached form," fish says. "It reads: 'From this point forward, reports will be submitted via the Internet. Print and fill out the attached Word document and fax it back to us.' "

Ch-ch-changes

Consultant pilot fish spends a month modeling a client's shift to a new change-management system. Then comes the big day to switch things over. "I flew 1,500 miles to babysit it," says fish. "But a systems tech – who also was a big fan of the old system – refused to allow the cutover to proceed. 'There is no change order in the system authorizing this,' he insisted. Of course, he was right. Nobody, including me, had thought to enter a change to change the change system."

CHANGE IS GOOD. But sending me your true tale of IT life at sharky@computerworld.com is better. You'll snag a snazzy Shark shirt if I use it. And check out Sharky's blog, browse the Sharkives and sign up for Shark Tank home delivery at computerworld.com/sharky.

FRANK HAYES ■ FRANKLY SPEAKING

Routed by Rootkits

CALL it the worst work-around ever. How else to describe the advice from Mike Danseglio, a Microsoft security guru, to wipe and reinstall Windows on any PC infected with an insidious malware known as a rootkit? Danseglio grabbed some headlines this month when he told an audience at the InfoSec World security conference that once a rootkit digs in, there's no sure way to get rid of it short of nuking Windows and starting from scratch.

But it turns out his suggestion isn't new. Danseglio's been giving that advice for most of a year. He wrote a Microsoft "Security Tip of the Month" that said the same thing last October.

And it's good advice. But as a work-around, it's terrible.

It's good advice because Danseglio's probably right: There's no other way to root out a rootkit. We can try to *prevent* infections — with firewalls, virus scanners, software patches and updates. But once a rootkit is in, it's in. It spreads its hooks everywhere. Rootkits are like cancer. You can cut out the obvious tumor, but there's no way to he absolutely sure you've removed every malignant cell from a patient's body.

We can't eliminate biological cancers with a wipe and reinstall. But we *can* get rid of rootkits that way. And if there's nothing better, it's a realistic tactical approach to the problem.

But it's still an awful work-around. Why? Because a work-around should be a trade-off, a rational decision about how to use resources. Work-arounds make sense when they cost less thao fixing underlying problems. But a work-around's cost piles up over time. Eventually you *do* want those underlying problems fixed.

In Windows, that's not going to happen. The rootkit vulnerabilities go to the core of Windows. They're not just bugs; they're flaws in Windows' basic design. Waiting for Microsoft to fix them is pointless. Microsoft doesn't have a fix, at least not short of entirely ripping out and replacing the guts of Windows.

And the only trade-off is that we foot the bill for Microsoft's years of failure to secure Windows.

Yes, some rootkits will he blocked by tighter security in Vista when it finally arrives — but not all rootkits. The soonest we can hope for a completely rearchitected, rootkit-proof Windows is literally years from now. And Microsoft has yet to promise anything like that.

FRANK HAYES, Computerworld's senior news columnist, has covered IT for more than 20 years. Contact him at frank_hayes@computerworld.com.

Meanwhile, we don't have just one work-around for the rootkit problem. We can actually try three different approaches.

Option A: Nuke and restore. You can automate the process. It might eveo become smooth — for IT. But don't underestimate the cost in lost productivity for users, who'll still have to adjust settings, rebuild their desktops and shortcuts, and reinstall their own applications (yes, they have them, even if they don't tell IT about them).

Option B: Change your Windows architecture. You can run Windows applications from a terminal server like Citrix. Or virtualize them with Softricity. Or move everything to blades. Yeah, it's a pricey traosition, and it'll shake up users. You'll also probably need a lot more network bandwidth. But rebuilding all those PCs will he easier if it's ever necessary.

Option C: Abandon Windows. Whether that means Web-based apps or Lioux or Macs or terminals, it's likely to be the most disruptive and costly option in the short term for both users and IT, and it will radically change what your IT shop does.

None of those options is a true trade-off. The cost and effort is all ours. We're facing complex and expensive choices, with no certainty that we'll ever see the underlying flaws fixed. Right oow, it's all Microsoft can do to fix surface-level problems like buffer overflows.

It's going to require a completely new Windows core to finally purge the rootkit cancer for good. And that's going to take a very hard, very expensive decision by Microsoft.

Not just the worst of work-arounds for us. ◗

What the @#$%! Is Wrong?

Spam filter catches an outgoing e-mail message with language that would make a sailor blush, and IT pilot fish forwards it to HR, as required by company policy. Turns out there's an explanation – sort of. "The employee said his home e-mail wasn't working, or so he thought," says fish. "So he drafted an expletive-filled missive at work and sent it to his home e-mail account. Not receiving it, he concluded that his home e-mail wasn't working and contacted his ISP. There really is no cure for stupid."

SHARK TANK

Aha!

Remote office can't access the system at headquarters one day, so HQ pilot fish tests the remote equipment. "Neither the router nor the CSU/DSU, which connects the office LAN to the dedicated circuit, could be located," says fish, who calls the phone company. Several hours later, telco calls back with the answer: "The smartjack, CSU/DSU, router, dumb terminal and printer were all gone," sighs fish. "Everything had been stolen."

Useless

User's personal mouse won't work with her laptop, and she demands that pilot fish fix it right away. "She said, 'Look, the laptop is not getting the information from the mouse,' " says fish. "I asked where the receiver to the wireless mouse was. She looked at me like I was an idiot. 'Isn't this a wireless laptop? Here's my wireless mouse. They should go together.' Again, I asked where the what-s-ma-thing with the black on-ble was. 'I got rid of the extra stuff,' says user. 'It wasn't needed.' "

One Step At a Time

State agency spends $300,000 to install high-speed Internet connections so local governments can file reports with the agency electronically, reports a pilot fish in the sale. "Finally, they send out an e-mail with an attached form," fish says. "It reads: 'From this point forward, reports will be submitted via the Internet. Print and fill out the attached Word document and fax it back to us.' "

Ch-ch-changes

Consultant pilot fish spends a month modifying a client's shift to a new change-management system. Then comes the big day to switch things over. "I flew 1,500 miles to babysit it," says fish. "But a systems tech – who also was a big fan of the old system – refused to allow the cutover to proceed. 'There is no change order in the system authorizing this,' he insisted. Of course, he was right. Nobody, including me, had thought to enter a change to change the change system."

CHANGE IS GOOD. But sending me your true tale of IT life at shanley@computerworld.com is better. You'll snag a snazzy Shark shirt if I use it. And check out Shanley's blog, browse the Sharkives and sign up for Shark Tank home delivery at computerworld.com/sharktank.

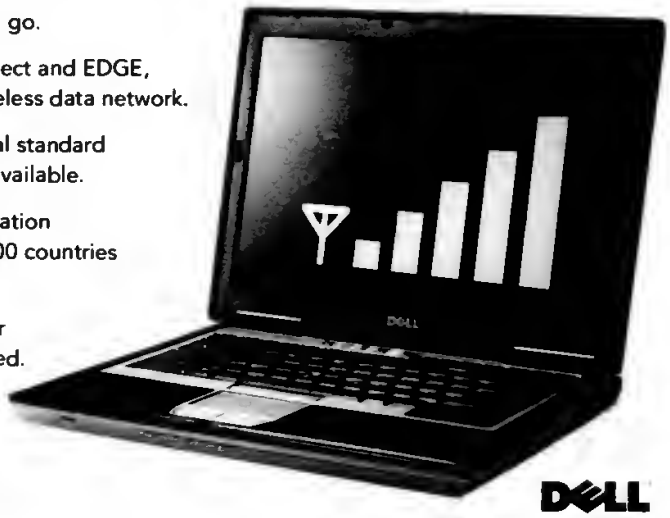
COMPUTERWORLD

INTRODUCING BUILT IN BroadbandConnect

the only built in wireless connection that works in more places than you do.

Get a Dell™ Latitude notebook equipped with Cingular's supercharged wireless network.

- Available on the Dell Latitude D620 and D820. Nothing to install. Just activate and go.
- Runs on Cingular's BroadbandConnect and EDGE, the largest national high-speed wireless data network.
- Broadband speeds on the 3G global standard everywhere BroadbandConnect is available.
- Access your business-critical information in 13,000 cities and towns and in 100 countries around the world.
- More secure than Wi-Fi with a wider coverage area – no hotspots required.



CINGULAR MAKES BUSINESS RUN BETTER

Click www.cingular.com/dell

cingular
raising the bar

Coverage not available in all areas. Cingular covers 273 million people. Wireless service not included with notebook. Other conditions and restrictions apply.